



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Yoshihiko Takagi et al.
Serial No.: 10/782,556
Filed: February 19, 2004
Title: "MEMORY DEVICE"
Docket No.: 36462

LETTER

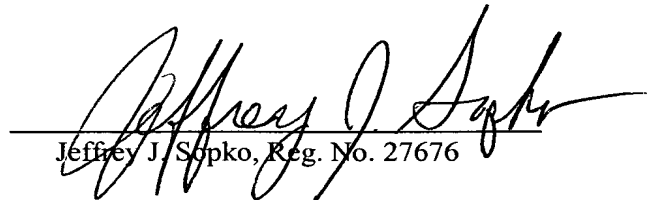
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Enclosed is a certified copy of Japan Patent Application No. 2003-042288, filed February 20, 2003; the priority of which has been claimed in the above-identified application.

Respectfully submitted,

PEARNE & GORDON LLP


Jeffrey J. Sopko, Reg. No. 27676

1801 East 9th Street
Suite 1200
Cleveland, Ohio 44114-3108
(216) 579-1700

March 16, 2004

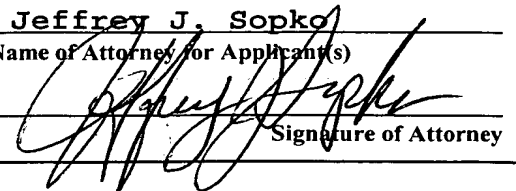
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, Va. 22313-1450 on the date indicated below.

Jeffrey J. Sopko

Name of Attorney for Applicant(s)

03/16/2004

Date


Signature of Attorney

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 2 0 日
Date of Application:

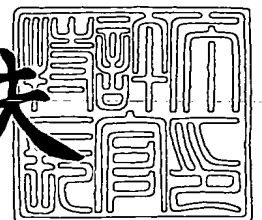
出 願 番 号 特 願 2 0 0 3 - 0 4 2 2 8 8
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 4 2 2 8 8]

出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):

2 0 0 4 年 2 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 0 5 5 8 7

【書類名】 特許願

【整理番号】 2030744066

【提出日】 平成15年 2月20日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 15/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 高木 佳彦

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 菊地 隆文

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100099254

【弁理士】

【氏名又は名称】 役 昌明

【選任した代理人】

【識別番号】 100100918

【弁理士】

【氏名又は名称】 大橋 公治

【選任した代理人】

【識別番号】 100105485

【弁理士】

【氏名又は名称】 平野 雅典

【選任した代理人】

【識別番号】 100108729

【弁理士】

【氏名又は名称】 林 紘樹

【手数料の表示】

【予納台帳番号】 037419

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9102150

【包括委任状番号】 9116348

【包括委任状番号】 9600935

【包括委任状番号】 9700485

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 メモリデバイス

【特許請求の範囲】

【請求項 1】 電子機器から直接アクセスすることができない耐タンパー性の第 1 のメモリと、電子機器から直接アクセスすることができない非耐タンパー性の第 2 のメモリとを備え、前記第 2 のメモリを使用して、前記第 1 のメモリに蓄積されたデータを退避することを特徴とするメモリデバイス。

【請求項 2】 退避するデータが、アプリケーションプログラムのインストール、または前記アプリケーションプログラムの実行によって生成されたデータであることを特徴とする請求項 1 に記載のメモリデバイス。

【請求項 3】 前記データを退避するとき、アプリケーションプログラムのプログラムコードを廃棄することを特徴とする請求項 2 に記載のメモリデバイス。

【請求項 4】 前記データを退避するとき、アプリケーションプログラムのプログラムコードを前記第 1 のメモリに残すことを特徴とする請求項 2 に記載のメモリデバイス。

【請求項 5】 退避するデータが、アプリケーションプログラムのインストール、または前記アプリケーションプログラムの実行によって生成されたデータと、前記アプリケーションプログラムのプログラムコードとであることを特徴とする請求項 1 に記載のメモリデバイス。

【請求項 6】 前記第 1 のメモリに蓄積されたデータの管理情報が格納された管理テーブルを具備し、前記管理情報に退避の可否を示す情報が含まれることを特徴とする請求項 1 に記載のメモリデバイス。

【請求項 7】 前記アプリケーションプログラムは、前記第 1 のメモリにダウンロードされてインストール処理されたものであることを特徴とする請求項 2 または 5 に記載のメモリデバイス。

【請求項 8】 前記アプリケーションプログラムは、前記第 2 のメモリにダウンロードされ、前記第 1 のメモリにインストール処理されたものであることを特徴とする請求項 2 または 5 に記載のメモリデバイス。

【請求項 9】 前記アプリケーションプログラムは、前記第 2 のメモリにダウンロードされ、前記第 2 のメモリにインストール処理されたものであることを特徴とする請求項 2 または 5 に記載のメモリデバイス。

【請求項 10】 退避するデータとその署名情報とを暗号化した上で、退避することを特徴とする請求項 1 に記載のメモリデバイス。

【請求項 11】 退避した情報を管理する退避情報管理手段を前記第 1 のメモリ内に備え、退避するデータを暗号化して退避し、前記暗号化されたデータの署名情報を前記退避情報管理手段へ保存することを特徴とする請求項 1 に記載のメモリデバイス。

【請求項 12】 電子機器からの指示に基づいて退避するデータを決定することを特徴とする請求項 1 または 6 に記載のメモリデバイス。

【請求項 13】 前記第 1 のメモリへのアプリケーションプログラムのダウンロードまたはインストールの指示を受けた際に、前記第 1 のメモリにダウンロードまたはインストールを行う余地が無いとき、前記第 1 のメモリに蓄積された退避可能なデータから任意のデータを退避させることを特徴とする請求項 1 に記載のメモリデバイス。

【請求項 14】 電子機器からの復元指示により、退避した特定のデータを復元することを特徴とする請求項 1 または 12 に記載のメモリデバイス。

【請求項 15】 電子機器からのアプリケーションプログラムの起動指示により、前記アプリケーションプログラムに関する退避データを復元することを特徴とする請求項 1 または 13 に記載のメモリデバイス。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、半導体メモリカードなどのメモリデバイスに関し、特に、秘匿性を備えた領域の効率的な活用を可能にするものである。

【0002】

【従来の技術】

近年、電子商取引などへの利用が拡大している IC カードは、耐タンパー性の

モジュール内にメモリ領域を有しており、そのため、データを強固に秘匿することができ、複製や偽造に対して固い耐性を備えている。しかし、ICカードのメモリ領域は、数十キロバイト程度の僅かなメモリ容量しか有していないため、多くのデータを格納することができない。

【0003】

このICカードに格納されたアプリケーションプログラム（以下、「AP」と言う）を一時的に端末に退避させて、ICカードを有効に活用する技術が下記特許文献1に記載されている。このICカードは、暗号化鍵を生成・管理し、退避対象のAPを暗号化してから端末に退避させる。また、退避させたAPを回復するときは、端末から受け取ったAPを、管理している暗号化鍵を用いて復号化し、ICカード内部のメモリ領域に再格納する。

【0004】

【特許文献1】

特開 2000-11101号

【0005】

【発明が解決しようとする課題】

しかし、ICカードに格納したAPを端末Aに退避させた場合は、その端末A以外の端末BでAPを利用しようとする、端末AをICカードに接続して、退避させたAPをICカード内部のメモリ領域に再格納し、その後に端末BとICカードとを接続したり、あるいは、端末Aに退避したAPを、ネットワーク等を介して端末Bに移送し、その後に端末BとICカードとを接続したりする必要がある。つまり、APをICカードの外に退避させた場合は、退避先の端末A以外の端末BでAPを利用する場合に、極めて煩雑な手順が必要になるという問題点がある。

【0006】

本発明は、こうした従来の問題点を解決するものであり、秘匿性を備えた領域を効率的に活用して、APの利用に必要な多くのデータを内部で安全に保持することができるメモリデバイスを提供することを目的としている。

【0007】

【課題を解決するための手段】

そこで、本発明のメモリデバイスには、電子機器から直接アクセスすることができない耐タンパー性の第1のメモリと、電子機器から直接アクセスすることができない非耐タンパー性の第2のメモリとを設け、第2のメモリを使用して、第1のメモリに蓄積されたデータを退避するように構成している。

このメモリデバイスでは、多数のAPの利用に必要なデータをデバイス内部で安全に保持することができるため、認証条件を満たす端末であれば、どの端末でも、そこに保持されたデータを利用することができる。

【0008】**【発明の実施の形態】**

本発明の実施形態における半導体メモリカード（ここでは「セキュアメモリカード」と呼ぶことにする）は、図2の概念図に示すように、耐タンパー性モジュール（tamper resistant module: TRM）40に含まれる内部CPU30及び内部不揮発性メモリ41と、非認証領域53、認証領域52及びセキュア領域51を備える大容量不揮発性メモリ50と、端末装置（リード/ライト（R/W）装置）の外部CPU60と通信して、端末装置によるメモリ領域へのアクセスを制御する制御部20とを備えている。

【0009】

内部不揮発性メモリ41及びセキュア領域51に対しては、内部CPU30のみがアクセス可能であり、端末装置は、内部不揮発性メモリ41及びセキュア領域51に直接アクセスすることはできない。また、制御部20は、端末装置の認証処理を行い、認証した外部CPU60が認証領域52にアクセスすることを許可する。一方、非認証領域53に対しては、端末装置は無条件でアクセスすることができる。

【0010】

TRM40の不揮発性メモリ41は、例えば、16バイト単位で消去・書き込みができるEEPROMから成り、また、大容量不揮発性メモリ50は、例えば、512バイト等のブロック単位での消去と1バイト単位での書き込みとが可能なフラッシュメモリから成る。

外部CPU60は、非認証領域53に無条件でアクセスすることができ、また、認証領域52には、制御部20での認証を済ませた場合にアクセスすることができるが、セキュア領域51及び内部不揮発性メモリ41の存在を知ることはできず、これらに直接アクセスすることはできない。

【0011】

セキュア領域51及び内部不揮発性メモリ41に対しては、内部CPU30だけがアクセス可能である。セキュア領域51と内部不揮発性メモリ41との違いは、内部不揮発性メモリ41がTRM40に設けられているのに対し、セキュア領域51が、耐タンパー性を持たない大容量不揮発性メモリ53に設けられている点である。そのため、セキュア領域51は、内部不揮発性メモリ41に比べて大きい蓄積容量を持つことができる。その反面、セキュリティレベルは、TRM40に設けられた内部不揮発性メモリ41よりも低い。この4つの領域のセキュリティレベルは、非認証領域53が最も低く、認証領域52、セキュア領域51、内部不揮発性メモリ41の順に高くなっている。

【0012】

図3のブロック図は、セキュアメモリカード10の構成を示している。セキュアメモリカード10は、大別して、制御部20と、大容量不揮発性メモリ50と、図2のTRM40に相当するIC部11とで構成される。大容量不揮発性メモリ50は、非認証領域53と、認証領域52と、セキュア領域51と、これらの領域のアドレス情報が格納されたアドレス情報管理領域54とを有している。

【0013】

制御部20は、R/W装置69との間でデータの授受を行うデータI/F部21と、R/W装置69との間でコマンドの授受を行うコマンドI/F部22と、R/W装置69を認証する制御認証部23と、受け付けたコマンドを解釈してコマンドに応じた処理を行う制御コマンド処理部24と、大容量不揮発性メモリ50へのアクセスを制御するとともにIC部11とのデータの受け渡し窓口となるアクセス制御部25と、大容量不揮発性メモリ50との間でデータを受け渡す大容量不揮発性メモリI/F部26とを備えている。

【0014】

また、耐タンパー性の IC 部 11 は、内部不揮発性メモリ 41 と、制御部 20 との間でデータやコマンドの授受を行う I/F 部 12 と、コマンドを解釈してコマンドに応じた処理を行う IC コマンド処理部 13 と、内部不揮発性メモリ 41 及びセキュア領域 51 にファイル形式で格納されたデータを管理するファイル管理部 14 と、R/W 装置 69 を認証し、認証した R/W 装置 69 に対して内部不揮発性メモリ 41 及びセキュア領域 51 へのデータアクセスを許可する IC 認証部 15 と、内部不揮発性メモリ 41 及びセキュア領域 51 への書き込み/読み出しデータに対して内部不揮発性メモリ 41 に格納された鍵を用いて暗号化/復号化を行う暗復号回路 17 と、内部不揮発性メモリ 41 及びセキュア領域 51 の管理を行うメモリ管理部 16 と、内部不揮発性メモリ 41 へのデータの授受を行う内部不揮発性メモリ I/F 部 18 とを備えている。

【0015】

制御部 20 の制御コマンド処理部 24 は、R/W 装置 69 から受信したコマンドを解釈し、そのコマンドが

- ・大容量不揮発性メモリ 50 の認証領域 52 または非認証領域 53 へのアクセスを要求するものであるか、
- ・認証を要求するものであるか、
- ・IC 部 11 による処理を要求するものであるか

を判断し、大容量不揮発性メモリ 50 の認証領域 52 または非認証領域 53 へのアクセスを要求しているときは、アクセス制御部 25 に大容量不揮発性メモリ 50 へのアクセス制御を指示し、IC 部 11 による処理を要求しているときは、アクセス制御部 25 に IC 部 11 へのコマンドの転送を指示し、また、認証を要求しているときは、制御認証部 23 に認証処理を指示する。

【0016】

アクセス制御部 25 は、大容量不揮発性メモリ 50 へのアクセス制御に当たって、大容量不揮発性メモリ 50 のアドレス情報管理領域 54 に記録されたアドレス情報を参照する。端末 (R/W 装置 69) が大容量不揮発性メモリ 50 の論理アドレスを指定してアクセスを求めて来たときは、アドレス情報管理領域 54 の記録から、指定されたアドレスが大容量不揮発性メモリ 50 のいずれの領域に属

しているかを判断し、認証領域 5 2 へのアクセス要求に対しては、認証済み端末に限って許可する。

【0017】

また、IC 部 1 1 の IC コマンド処理部 1 3 は、制御部 2 0 から送信されたコマンドを解釈し、その処理要求が、

- ・内部不揮発性メモリ 4 1 へのデータ書き込み／読み出しを要求するものであるか、
- ・セキュア領域 5 1 へのデータ書き込み／読み出しを要求するものであるか、
- ・認証を要求するものであるか、
- ・その他の処理を要求するものであるか

を判断する。

【0018】

コマンドが、認証を要求しているときには、IC コマンド処理部 1 3 は、IC 認証部 1 5 に R/W 装置 6 9 の認証処理を指示する。

また、コマンドが、内部不揮発性メモリ 4 1 へのデータの書き込み／読み出し、または、セキュア領域 5 1 へのデータの書き込み／読み出しを要求するコマンドであるときには、IC コマンド処理部 1 3 は、IC 認証部 1 5 において認証処理が済んでいるかを確認し、認証処理が済んでいる場合は、その要求を許可し、その要求が書き込み要求であるときは、書き込むデータを、格納先の情報を付してメモリ管理部 1 6 に送る。

【0019】

内部不揮発性メモリ 4 1 及びセキュア領域 5 1 を管理するメモリ管理部 1 6 は、書き込むデータを暗復号回路 1 7 で暗号化し、データに署名（この処理に用いる暗号鍵や検証鍵は内部不揮発性メモリ 4 1 に格納されている）を付した後、内部不揮発性メモリ 4 1 に書き込むべきデータを、内部不揮発性メモリ I/F 部 1 8 を介して、内部不揮発性メモリ 4 1 に書き込み、書き込み位置の情報をファイル管理部 1 4 に伝える。また、セキュア領域 5 1 に書き込むべきデータを、大容量不揮発性メモリ I/F 部 2 6 を介して、大容量不揮発性メモリ 5 0 のセキュア領域 5 1 に書き込み、書き込み位置の情報をファイル管理部 1 4 に伝える。なお

、署名は、暗号化したデータとは別に内部不揮発性メモリ 41 で保持する場合もある。

【0020】

ファイル管理部 14 は、メモリ管理部 16 から伝えられた情報を基に、内部不揮発性メモリ 41 及びセキュア領域 51 に格納されたファイルを管理する。

また、IC コマンド処理部 13 は、その要求が読み出し要求であるときは、読み出すべきデータのファイル位置をファイル管理部 14 に求め、メモリ管理部 16 にそのファイルの読み出しを要求する。

メモリ管理部 16 は、そのファイルを内部不揮発性メモリ 41 またはセキュア領域 51 から読み出すと、暗復号回路 17 でデータの署名検証や復号化を行い、IC コマンド処理部 13 に送る。

【0021】

復号化されたデータは、制御部 20 に送られ、データ I/F 部 21 から R/W 装置 69 に送信される。

また、IC コマンド処理部 13 は、メモリ容量が少ない内部不揮発性メモリ 41 を有効に活用するため、内部不揮発性メモリ 41 に格納したデータをセキュア領域 51 に退避させる処理を行う。以下、この退避処理について詳しく説明する。

【0022】

(第 1 の実施形態)

IC コマンド処理部 13 は、端末から、セキュアカード内部で動作する、退避可能な AP のダウンロード (以下「DL」と言う) が要求された場合に、内部不揮発性メモリ 41 に空きが有るときは、端末から送られた AP のプログラムコード (プログラムを記述するプログラムデータ) を内部不揮発性メモリ 41 に格納する処理、即ち、DL 処理を行う。また、端末のインストール要求に応じて、DL した AP のプログラムコードを実行し、AP 用のデータを作成して AP を実行可能な状態にする処理、即ち、インストール処理を行う。

【0023】

また、IC コマンド処理部 13 は、内部不揮発性メモリ 41 に空きが無いとき

は、端末からの指示により（または、自らの判断で）、内部不揮発性メモリ 4 1 に既に格納されている、退避可能な A P のプログラムコード及びデータをセキュア領域 5 1 に退避させる処理を行い、空きができた内部不揮発性メモリ 4 1 に、端末から送られた A P の D L 処理及びインストール処理を行う。

また、I C コマンド処理部 1 3 は、セキュア領域 5 1 に退避した A P の起動が端末から要求された場合に、その A P をインストール状態に戻すために、内部不揮発性メモリ 4 1 に空いた領域が有るときは、起動要求された A P のプログラムコード及びデータを内部不揮発性メモリ 4 1 に復元（データ移動）し、その A P を起動する。

【0024】

この場合、内部不揮発性メモリ 4 1 に空いた領域が無いときは、内部不揮発性メモリ 4 1 に格納されている退避可能な A P のプログラムコード及びデータをセキュア領域 5 1 に退避させ、空きができた内部不揮発性メモリ 4 1 に、起動要求された A P のプログラムコード及びデータを復元する。

なお、セキュア領域 5 1 への退避は、A P のインストール処理で作成したデータだけを対象に行い、A P のプログラムコードについては内部不揮発性メモリ 4 1 から削除するようにしても良い。プログラムコード自体は、退避するデータと違って、セキュアカードで生成したものではなく、いつでも端末から同じものを D L することが可能なためである。この A P の起動は、セキュア領域 5 1 に退避した A P のデータを内部不揮発性メモリ 4 1 の空き領域に復元し、端末から A P のプログラムコードを内部不揮発性メモリ 4 1 に D L して行われる。

【0025】

図 1 は、この内部不揮発性メモリ 4 1 の構成を示している。内部不揮発性メモリ 4 1 の内部には、A P のプログラムコードが格納される A P 格納領域 4 1 1 と、A P で利用するデータが格納されるデータ格納領域 4 1 2 と、内部不揮発性メモリ 4 1 にプログラムコード及びデータが格納された A P を管理するための A P 管理テーブル 4 1 3 と、セキュア領域 5 1 に退避した A P を管理するための退避 A P 管理テーブル 4 1 4 と、退避・復元するコードやデータの暗号化・復号化に用いる鍵と署名生成・検証に用いる鍵とが格納された鍵管理領域 4 1 5 とが設け

られている。

【0026】

AP管理テーブル413には、図4に示すように、APがどのようなものであるかを一意に示すAP識別子と、そのAPのインストール処理がされているか否かを示すインストールフラグと、プログラムコードが格納されたAP格納領域411のアドレスを示すコードアドレスと、データが格納されたデータ格納領域412のアドレスを示すデータアドレスと、このAPが退避可能であるか否かを示す退避可否とが記述される。なお、退避可否は、APのDL時に端末から伝えられる。

【0027】

また、退避AP管理テーブル414には、図5に示すように、AP識別子と、退避させたデータの格納位置等を一意に特定するための退避データ識別子と、退避データに対する署名データとが記述される。退避データ識別子は、様々な形式で設定することができ、例えば（退避先アドレス+データサイズ）を退避データ識別子としても良い。

また、図6には、退避データを格納するデータ退避領域511を備えたセキュア領域51の構成を示している。

【0028】

次に、APのDL、インストール、退避、及び復元に伴うAP管理テーブル413や退避AP管理テーブル414の遷移について説明する。

図13(a)には、初期状態（APが1つもDL/インストール/退避/復元されていない状態）のAP管理テーブル413を示し、また、図16(a)には、初期情報の退避AP管理テーブル414を示している。端末からAPとして退避可否が可のAP1がDLされると、AP管理テーブル413には、図13(b)のように記述される。「code1」は、AP格納領域411に格納されたAP1のプログラムコードのアドレスを示している。さらに、退避可否が可のAP2がDLされると、AP管理テーブル413の記述は図13(c)のようになる。AP1及びAP2をインストールした状態では、AP管理テーブル413の記述は図14(d)のように変わり、データ格納領域412に格納されたAP1の

データのアドレスが「data1」として、データ格納領域412に格納されたAP2のデータのアドレスが「data2」として記述される。

【0029】

図14(e)には、さらに、端末から退避可否が否のAP3、退避可否が可のAP4及びAP5がDLされ、インストールした状態を示している。また、このときの内部不揮発性メモリ41のAP格納領域411及びデータ格納領域412の状態を図17(a)に、セキュア領域51のデータ退避領域511の状態を図17(b)に示している。AP格納領域411には空きが無い。

次に、このようにAP格納領域411に空きが無い状態で、端末があるAP(ここではAP6)のDLを要求した場合には、端末とICコマンド処理部13との間で図7に示す処理が行われる。

【0030】

端末がAP6のDLを要求すると(①)、ICコマンド処理部13は、内部不揮発性メモリ41のAP格納領域411に空きが存在しないため、空き領域がない旨のエラー通知を端末に対して行う(②)。端末は、退避可能なAP一覧を要求し(③)、カードから退避可能なAP一覧を取得して(④)、その中から退避可能なAP(ここではAP2)を選択して、AP2の退避を要求する(⑤)。ICコマンド処理部13は、AP2の退避処理を行い(⑥)、退避完了通知を端末に伝える(⑦)。AP2の退避処理が行われた状態でのAP管理テーブル413を図15(f)に示し、退避AP管理テーブル414を図16(b)に示し、また、内部不揮発性メモリ41のAP格納領域411及びデータ格納領域412の状態を図18(a)に、セキュア領域51のデータ退避領域511の状態を図18(b)に示している。

【0031】

端末はAP6のDLを要求し(⑧)、ICコマンド処理部13は、AP6のDL処理を行い(⑨)、DL完了通知を端末に送る(10)。AP6のDL処理が行われた状態でのAP管理テーブル413を図15(g)に示し(アドレスcode6は、AP2の退避により空き領域となったcode2またはdata2と同一となることもあるし、ならないこともある)、また、内部不揮発性メモリ41

のAP格納領域411及びデータ格納領域412の状態を図20(a)に示している。

【0032】

なお、ここでは、ICコマンド処理部13が端末からのAP退避要求を待って退避処理を行う場合について示したが、AP格納領域411に空きが無いときに、ICコマンド処理部13が自ら判断してAPの退避処理を行うことも可能である。この場合、図8に示すように、端末がAP6のDLを要求すると(①)、ICコマンド処理部13が、退避可能なAPの中から選択したAP2を退避させて(②)、AP格納領域411に空き領域を確保した後、AP6のDL処理を行い(③)、DL完了通知を端末に送る(④)、と言う処理手順になる。

このように、端末に意識されることなく、自動的に退避処理が行われる。また、この場合、AP6のDL完了後、AP2を自動的に退避させたことを端末に通知するようにしても良い。

【0033】

また、図7の⑥、あるいは、図8の②でのAP退避処理は、図9(a)または図9(b)に示す手順で実行される。図9(a)は、署名データをセキュア領域51に格納する方式であり、まず、署名鍵を用いて、退避用データ(前述するように、インストール処理されたAPのプログラムコードと生成データとを退避用データにする場合と、生成データだけを退避用データにする場合とがある)の署名データを生成し(①)、退避用データと署名データとを連結し(②)、連結したデータを退避用暗号鍵で暗号化し(③)、暗号化したデータをセキュア領域51のデータ退避領域511に格納する(④)。そして、退避AP管理テーブル414にAP識別子及び退避データ識別子を追加する(この方式の場合には、署名データは、退避AP管理テーブル414に加えない)。インストール処理で生成したデータだけを退避用データとした場合は、AP格納領域411から退避対象APのプログラムコードを削除し、AP管理テーブル413上から退避対象APに関する情報を削除する。

【0034】

一方、図9(b)は、署名データを退避AP管理テーブル414に保存する方

式であり、退避用データを暗号鍵で暗号化し (①)、署名鍵を用いて暗号化データの署名データを生成し、この署名データを退避AP管理テーブル414に保存する (②)。暗号化したデータはセキュア領域51のデータ退避領域511に格納する (③)。そして、退避AP管理テーブル414に、さらにAP識別子及び退避データ識別子を追加する。インストール処理で生成したデータだけを退避用データとした場合は、AP格納領域411から退避対象APのプログラムコードを削除し、AP管理テーブル413上から退避対象APに関する情報を削除する。

【0035】

次に、端末が、退避状態のAP2に対して起動要求した場合のセキュアカード10の動作について説明する。この場合、AP2が退避されていることを端末が認識し、端末からAP2の復元要求を行う方法と、ICコマンド処理部13が、起動要求されたAP2の退避を認識し、自らAP2の復元処理を行う方法とがある。

【0036】

図10には、端末からAP2の復元要求を行う場合の手順を示している。端末はAP2の起動要求をセキュアカード10に対して行う (①)。ICコマンド処理部13は、AP管理テーブル413を参照してAP2が内部不揮発性メモリ41に存在しないことを認識し (②)、端末にAP2が内部不揮発性メモリ41に存在しないことを通知する (③)。端末はセキュアカード10に「退避AP管理テーブル」414の取得を要求し (④)、ICコマンド処理部13は、端末に退避AP管理テーブル414を送信する (⑤)。端末は退避AP管理テーブルによってAP2が退避されていることを認識し、セキュアカード10に任意のAP (ここではAP4) の退避要求を行う (⑥)。ICコマンド処理部13は、AP4の退避処理を行い (⑦)、端末に退避完了を通知する (⑧)。

【0037】

図19には、図20の状態からAP4を退避させたときのAP格納領域411、データ格納領域412及びデータ退避領域511の状態を示し、また、図16(c)には、このときの退避AP管理テーブル414を示している。

次いで、端末はセキュアカード10にAP2の復元要求を行う(⑨)。ICコマンド処理部13は、AP2の復元処理を行い(10)、端末に復元完了を通知する(11)。図15(h)は、AP2を復元処理した状態のAP管理テーブル413を示し(アドレスcode7及びdata7は、AP4の退避により空き領域となったcode4またはdata4と同一となることもあるし、ならないこともある)、また、図16(d)は、このときの退避AP管理テーブル414を示し、図21は、このときのAP格納領域411、データ格納領域412及びデータ退避領域511の状態を示している。

次いで、端末はセキュアカード10に再度AP2の起動要求を行う(12)。ICコマンド処理部13は、AP2を起動し(13)、端末に起動完了を通知する(14)。

【0038】

なお、③の通知において、同時に、AP2が退避中であることを通知することによって、④、⑤を省略することもできる。また、AP2が退避中であることを端末が認識している場合には、④以降の手順が行われる。また、AP2の退避がインストール処理で生成されたデータについてのみ行われ、AP2のプログラムコードが削除されている場合には、端末は、⑨の手順でAP2のプログラムコードをDLする。

【0039】

一方、図11は、ICコマンド処理部13が、起動要求されたAP2の退避を認識し、自らAP2の復元処理を行う場合の手順を示している。端末はAP2の起動要求をセキュアカード10に対して行う(①)。ICコマンド処理部13は、AP管理テーブル413を参照してAP2が内部不揮発性メモリ41に存在しないことを認識し、次に、退避AP管理テーブル414を参照してAP2が退避されていることを認識し、あるAPを退避対象として選択し(ここではAP4)、その退避処理を行う。次いで、空いた領域にAP2を復元し(②)、AP2を起動して(③)、端末には起動完了を通知する(④)。

【0040】

この場合、AP2が退避されていることを気付いていない端末が、AP2の起

動指示を出した場合でも、そのAP2を起動するための処理が、ICコマンド処理部13によって行われる。そのため、端末は、起動要求するAPが退避されているか否かを意識する必要がない。

なお、この方法は、AP2の退避がインストール処理で生成されたデータについてのみ行われ、AP2のプログラムコードが削除されている場合には、適用できない。

【0041】

また、図10の(10)、あるいは、図11の②での復元処理は、退避処理が図9(a)の手順で行われているときは、図12(a)の手順で、また、退避処理が図9(b)の手順で行われているときは、図12(b)の手順で行われる。図12(a)では、退避AP管理テーブル414のAP識別子により退避データ(暗号化データ)を認識し、復号鍵を用いて暗号化データを内部不揮発性メモリ41上に復号化する(①)。次いで、復号化したデータから退避データ本体と署名データとを認識し、検証鍵を用いて、署名データの正当性を検証する。署名が正当であるときは、退避データ本体に含まれるプログラムコードを内部不揮発性メモリ41のAP格納領域411に、データをデータ格納領域412に復元する(②)。また、AP管理テーブル413にAP識別子を記述し、インストールフラグをONに設定し、AP格納領域411及びデータ格納領域412に格納した復元データのアドレスをコードアドレス及びデータアドレスとして記述する。最後にセキュア領域51内の退避暗号化データと、退避AP管理テーブル414の当該APに関する部分を削除する。

【0042】

また、図12(b)の手順では、退避AP管理テーブル414のAP識別子により退避データ(暗号化データ)を認識し、検証鍵を用いて、退避AP管理テーブル414に記述された署名データとの検証を行う(①)。検証結果が正常であれば、復号鍵を用いて暗号化データを内部不揮発性メモリ41上に復号し(②)、プログラムコードを内部不揮発性メモリ41のAP格納領域411に、また、データをデータ格納領域412に復元する(③)。その後の処理は図12(a)の場合と同じである。

【0043】

また、APの退避がインストール処理で生成されたデータについてのみ行われている場合には、端末がAPのプログラムコードをDLしたときに、データの復元処理が次の手順で行われる。

復元対象APを端末からDLする。ICコマンド処理部13は、AP管理テーブル413にAP識別子及びコードアドレスを記述し、DLしたAPと同一のAP識別子を退避AP管理テーブル414より検索する。対応するものが存在すれば、セキュア領域51のデータ退避領域511から暗号化データを読み出し、復号化する。復号化したデータから、退避データ本体と署名データとを認識し、署名データの正当性の検証を行う。検証結果が正当であれば、退避データ本体を内部不揮発性メモリのデータ格納領域412に格納し、AP管理テーブル内の該当するAPのインストールフラグをONに設定し、データアドレスとして、復元データを格納したデータ格納領域412のアドレスを設定する。最後にセキュア領域内の退避暗号化データと、退避AP管理テーブルの該APに関する部分を削除する。

【0044】

ここでは、APのプログラムコードと、インストール処理で生成されたデータとを共に退避する場合、及び、データのみを退避し、プログラムコードを削除する場合について説明したが、プログラムコードに比べてデータのデータ量が遥かに大きい場合には、データのみをセキュア領域51に退避し、プログラムコードは、内部不揮発性メモリ41のAP格納領域411に残しておくことも可能である。こうした方式を採ると、図18に示すAP格納領域411、データ格納領域412及びデータ退避領域511の状態は、図22のように変わり、また、図20に示す状態は、図23のように変わる。

【0045】

APのプログラムコード及びデータを共に退避する場合、並びに、データを退避し、プログラムコードを内部不揮発性メモリに残す場合には、図11に示す、ICコマンド処理部による自動的な復元処理手順が可能となる。

また、端末から、セキュア領域51に退避中のAPの起動が要求されたとき、

次の手順により、APのプログラムコードやデータをセキュア領域51に置いたまま、APの実行を行うことも可能である。

【0046】

例えば、図18、図15(f)及び図16(b)の状態にあるとき、端末がセキュアカード10に対しAP2の実行を要求すると、ICコマンド処理部13は、AP管理テーブル(図15(f))よりAP2がインストール状態でないことを認識し、退避AP管理テーブル(図16(b))より退避中であることを認識し、退避データ識別子により、evac2を読み出し、復号化と署名検証とを行う。署名検証が正常に終了すると、復号化データよりAP2のプログラムコードを取得し、AP2の実行を行う。

この場合には、退避中のAPを内部不揮発性メモリ41に復元することを要しない。

【0047】

このように第1の実施形態のセキュアメモリでは、内部不揮発性メモリにDLされてインストール処理されたAPの内、退避の可能なものだけが退避される。そのため、最高度の機密を要するAPは、「退避不可」とすることにより、退避の対象から外れることができる。また、紛失の危険性を甘受できる程度のセキュリティを要求するAPは、「退避可」とすることにより、セキュアメモリにおける秘匿領域の効率的な利用が可能になる。

【0048】

(第2の実施形態)

本発明の第2の実施形態におけるセキュアメモリの構成は、第1の実施形態(図2、図3)と同じである。

第1の実施形態では、APをセキュアメモリ10の内部不揮発性メモリ41にDLし、内部不揮発性メモリ41に新たなAPをDLする空きが無いときに、インストール処理された退避可のAPを内部不揮発性メモリ41からセキュア領域51に退避させる場合について説明したが、第2の実施形態では、セキュア領域51をAPのDL先とすることを可能にしている。ただし、セキュア領域51にDLされたAPのインストール処理は、内部不揮発性メモリ41で行われる。

【0049】

APのDL先を内部不揮発性メモリ41とするか、セキュア領域51とするかは、次のような方式で決定される。

第1の方式では、DL時に、APのプログラムコードと合わせて、端末から内部不揮発性メモリDL専用フラグを送信する。セキュアメモリ10のICコマンド処理部13は、そのフラグを参照し、内部不揮発性メモリDL指定がなされていれば、必ず内部不揮発性メモリ41にDLし、内部不揮発性メモリDL指定がなされていない場合は、内部不揮発性メモリ41に空きがあるときは、内部不揮発性メモリ41にDLし、内部不揮発性メモリ41に空きが無いときは、セキュア領域51にDLする。

【0050】

また、第2の方式では、端末がセキュア領域51へのDLを許可する場合のみ、DL時にAPのプログラムコードと合わせて、セキュア領域DL許可フラグを送信する。セキュアメモリ10のICコマンド処理部13は、セキュア領域DL許可フラグが付加されていれば、内部不揮発性メモリ41に空きがあるときは、内部不揮発性メモリ41に、内部不揮発性メモリ41に空きが無いときは、セキュア領域51にDLし、セキュア領域DL許可フラグが付加されていない場合は、必ず内部不揮発性メモリ41にDLする。

このセキュアメモリ10のセキュア領域51は、図24に示すように、データ退避領域511の他に、DLされたAPのプログラムコードを格納するAP保存領域512を備えている。

【0051】

また、内部不揮発性メモリ41は、図1と同様の構成を備えている。ただし、AP管理テーブルは、図25に示すように、内部不揮発性メモリ41にDLまたはインストールされた状態のAPを管理するためのAP管理テーブル413と、セキュア領域51にDLされたAPを管理するためのセキュア領域DLAP管理テーブル416とから成る。セキュア領域DLAP管理テーブル416には、APを内部不揮発性メモリ41上でインストールするために必要となる事項、即ち、APが格納されているセキュア領域51上の位置を示す「格納アドレス」、そ

のAPの改ざんの有無を確認するための「署名データ」、そのAPがインストール後に退避可能か否かを示す「退避可否フラグ」がAP識別子と共に記述される。

【0052】

AP管理テーブル413の項目は、第1の実施形態（図4）と同じであり、内部不揮発性メモリ41上に格納されたAPが、インストール状態であるか否かを示す「インストールフラグ」、退避可能か否かを示す「退避可否フラグ」、インストール状態であるときのデータの所在を示す「データアドレス」、及び、プログラムコードの読み出し先を示す「コードアドレス」がAP識別子と共に記述される。

【0053】

このAP管理テーブル413の特定番号、例えば#4及び#5は、セキュア領域51にDLされたAP（セキュア領域DLAP）のインストール用に確保されており、内部不揮発性メモリ41へのAPのDLには、そこを使用することができない。そのため、内部不揮発性メモリ41にDLするAPのDL及びインストール処理は、AP管理テーブル413の#1～#3を使って、第1の実施形態と同じように行われる。

【0054】

一方、セキュア領域51にDLしたAPに対して、ICコマンド処理部13は、次の手順でインストールを行う。

セキュア領域DLAP管理テーブル416の格納アドレスにしたがって、セキュア領域51のAP保存領域512からAPのプログラムコードを読み出し、復号化及び署名検証を行う。検証結果が正常であれば、復号化したプログラムコードを内部不揮発性メモリ41のAP格納領域411に格納し、AP管理テーブル413のセキュア領域DLAP用の特定番号にAP識別子、コードアドレス、退避可否フラグ（セキュア領域DLAP管理テーブル416に記述されているものと同じもの）を設定する。

このとき、セキュア領域DLAP用の特定番号に空きが無ければ、この特定番号を使用しているインストール済みのAPをセキュア領域51のデータ退避領域

511に退避させて、空きを作る。

【0055】

次いで、ICコマンド処理部13は、インストール処理を行い、作成したデータをデータ格納領域412に格納し、AP管理テーブル413にデータアドレスを記述し、インストールフラグをONにする。

このインストール後もセキュア領域51にDLされたAPのプログラムコードは、セキュア領域51のAP保存領域512にそのまま存在し、セキュア領域DLAP管理テーブル416の記述は残される。そのため、インストールしたAPの退避処理に伴ってプログラムコードが削除されても、端末からの再DLは必要が無い。

【0056】

内部不揮発性メモリへのDLを指定するAP（内部不揮発性メモリDL専用AP）は、セキュア領域への退避を好まない。一方、セキュア領域へのDLが可能なAP（セキュア領域DL可能AP）は、退避を行うことに問題がないと考えられる。このセキュアカードでは、セキュア領域にDLしたAPと内部不揮発性メモリにDLしたAPとを分けて管理しているため、内部不揮発性メモリDL専用APが格納される領域は、セキュア領域DL可能APによって埋められてしまうことはなく、一方、セキュア領域DL可能APは、専用の領域が確保されているので、インストール状態にあるセキュア領域DL可能APを退避させることで別のセキュア領域DL可能APをインストールすることが可能となる。

【0057】

なお、AP管理テーブル413の分け方は、例えば#1～#3は内部不揮発性メモリDL専用AP向け、#4～#5はどちらでもよいAP向け、というような区分でも良い。

また、セキュア領域にDLしたAPのみを退避可能とし、内部不揮発性メモリにDLしたAPは退避不可とすることも可能である。この場合には、セキュア領域DLAP管理テーブルの退避可否フラグは無くてもよい。

また、セキュア領域DLAP管理テーブルに、インストールフラグ及びデータ格納アドレスを追加することで、セキュア領域へのインストール（データ格納領

域の生成)を行うこともできる。

【0058】

ここで示した、内部不揮発性メモリへのDLを指定するAPには、セキュリティが高いもの、例えば電子マネーAPなどが該当するであろう。このような直接金銭に絡む、セキュリティ強度が要求されるAPは、内部不揮発性メモリの外にプログラムコード及びデータを出すことが望ましくない。そのため、退避不可と設定されることが考えられる。

【0059】

また、ICカード(セキュアメモリカードのIC部を含む)の利用が一般に広まるにつれて、厳密な手続きを行わずに任意のプレイヤーがAPをカードにインストールすることが可能になるものと考えられる。そうすると、いずれかのサーバにアクセスする際(または、何らかの端末アプリケーションを使用する際)に必要なIDとパスワードとを管理するAP等は、セキュア領域DL可能APになると考えられる。そのサーバが事業者または個人によって運用される場合(特に個人が運用するサーバの場合)には、さほどセキュリティレベルは要求されず、万一IDとパスワードとを紛失した(壊れた)場合でも、容易に再発行が可能である。

【0060】

このようなAPに対して、電子マネーAPと同等に、容量の小さい内部不揮発性メモリを常時利用させることは、コスト面から望ましくない。それよりも、大容量のセキュア領域にDLし、同じようにセキュア領域にDLしたAPを使用する際に退避されるという運用方法が妥当である。

ただ、このような仕分けは、論理必然的に導かれるものではなく、AP提供者が希望するセキュリティ要求度とカード発行者が判断する内部不揮発性メモリ利用の妥当性とにより様々に設定されることになる。

【0061】

いずれにしろ、第2の実施形態のセキュアカードでは、セキュア領域へのDLが可能であるため、第1の実施形態に比べて、APのDL処理及びインストール処理における、より多くのパターンが選択できる。そのため、APの種々のセキ

セキュリティ要求レベルに対応することが可能であり、セキュアメモリの秘匿領域を、より効率的に利用することができる。

【0062】

また、さらに、APのセキュア領域へのDLとともに、セキュア領域へのインストール処理を可能にすれば、APのDL処理及びインストール処理におけるパターンは一層増加し、セキュアメモリの秘匿領域をさらに効率的に利用することができる。例えば、内部不揮発性メモリにDLされ、内部不揮発性メモリにインストール処理された高度セキュリティのAPと、セキュア領域にDLされ、内部不揮発性メモリにインストール処理された準高度セキュリティのAPとを退避不可とし、セキュア領域にインストール処理されたAPを退避可とすることなども可能になる。

【0063】

(第3の実施形態)

本発明の第3の実施形態では、AP間で共用するデータが退避中である場合のデータの利用について説明する。

AP間でデータの共有が可能な仕組みを持ち、AP2が許可したAP（ここではAP1）は、AP2のデータを参照することが可能であるものとする。許可対象AP（AP1）は、許可する側のAP（AP2）により管理されたデータのうち、特定のデータ（一部のデータ）に対してのみ参照することが可能であり、また、そのような一部のデータに対する他APからの参照許可を複数設定することが可能であるものとする。

【0064】

図26(a)には、あるAPが参照許可を与えたデータと許可対象APとの関係を記述した許可指定テーブルの例を示しており、ここでは、図26(b)に示すように、AP1に対してdata_aの参照許可が設定されているものとする。また、図18、図15(f)及び図16(b)に示すように、AP1がインストール状態、AP2が退避状態とする。

【0065】

ICコマンド処理部13は、AP2の退避処理において、データの退避時に許

可対象のデータ `data_a` も含めて退避させる。AP1の実行時に、AP2が保持するデータ `data_a` への参照が発生すると、ICコマンド処理部13は、AP管理テーブル（図15（f））よりAP2がインストール状態にないことを認識し、退避AP管理テーブル（図16（b））よりAP2が退避状態であることを認識し、退避中のAP2の暗号化データ `evac2` を読み出し、復号化と署名検証とを行い、検証が正常に終了すれば、復号化したAP2のデータから `data_a` を参照する。

【0066】

また、`data_a` への書き込みが発生する場合は、更新した `data_a` とともにAP2のデータ全体に対して暗号化、署名生成を行い、暗号化データのセキュア領域への格納とともに、格納先を示す `evac2` を更新し、署名データ `sign2` を、生成した署名データに更新する。

また、データと同様に、退避中のAPのプログラムコードを他のAPで利用することも可能である。図27（a）（b）には、あるAPが実行許可を与えるプログラムコードと許可対象APとの関係を記述した許可指定テーブルの例を示している。前述するデータと同様の手順で、AP1は、退避中のAP2の `code_a` を実行することができる。

【0067】

なお、第1の実施形態で示したように、APの退避には、

- ①データのみ退避+プログラム削除
- ②データ+プログラムをともに退避
- ③データのみ退避、プログラムを内部不揮発性メモリに残す

の3パターンがある。第2の実施形態でセキュア領域DL可能APに該当するものとして示したサーバへのアクセスに利用するAPの場合、利用時にネットワークに接続されるので、プログラムコードのDLが可能であるため、①のパターンが適する（②や③の適用を否定するものではない）。

また、端末APを使用する際に必要なIDとパスワードとを管理するようなAPの場合には、常にネットワークに接続されている訳ではないため、②のパターンが適している（③の適用を否定するものではない）。なお、③については、A

P 提供者がプログラムコードの退避を望まない場合に適用し得る。

【0068】

なお、本発明の実施形態では、大容量不揮発性メモリ 50 に、記憶領域として、非認証領域、認証領域及びセキュア領域の 3 領域を設けた例を示しているが、本発明では、大容量不揮発性メモリ 50 に、セキュア領域を備えることが必要であって、その他の領域については問わない。

【0069】

【発明の効果】

以上の説明から明らかなように、本発明のセキュアカードは、秘匿性を備えた領域を効率的に活用して、多数の AP の利用に必要なデータを内部で安全に保持することができる。そのため、認証条件を満たす端末であれば、どの端末でも、セキュアカードに保持されたデータを利用することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリの構成を示す図

【図 2】

本発明の第 1 の実施形態におけるセキュアカードの概略図

【図 3】

本発明の第 1 の実施形態におけるセキュアカードの構成を示すブロック図

【図 4】

本発明の第 1 の実施形態におけるセキュアカードの AP 管理テーブルの構成を示す図

【図 5】

本発明の第 1 の実施形態におけるセキュアカードの退避 AP 管理テーブルの構成を示す図

【図 6】

本発明の第 1 の実施形態におけるセキュアカードのセキュア領域の構成を示す図

【図 7】

本発明の第 1 の実施形態におけるセキュアカードの退避シーケンスを示す図（端末からトリガを掛ける場合）

【図 8】

本発明の第 1 の実施形態におけるセキュアカードの退避シーケンスを示す図（カード自身が判断して退避させる場合）

【図 9】

本発明の第 1 の実施形態におけるセキュアカードの退避データ生成手順を示す図

【図 10】

本発明の第 1 の実施形態におけるセキュアカードの復元シーケンスを示す図（端末から復元トリガを掛ける場合）

【図 11】

本発明の第 1 の実施形態におけるセキュアカードの復元シーケンスを示す図（カード自身が自動で復元する場合）

【図 12】

本発明の第 1 の実施形態におけるセキュアカードの復元データ生成手順を示す図

【図 13】

本発明の第 1 の実施形態におけるセキュアカードの AP 管理テーブルの推移を示す図（a～c）

【図 14】

本発明の第 1 の実施形態におけるセキュアカードの AP 管理テーブルの推移を示す図（d～e）

【図 15】

本発明の第 1 の実施形態におけるセキュアカードの AP 管理テーブルの推移を示す図（f～h）

【図 16】

本発明の第 1 の実施形態におけるセキュアカードの退避 AP 管理テーブルの推

移を示す図

【図 17】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 1）

【図 18】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 2）

【図 19】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 3）

【図 20】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 4）

【図 21】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 5）

【図 22】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 6）

【図 23】

本発明の第 1 の実施形態におけるセキュアカードの内部不揮発性メモリ及びセキュア領域の推移を示す図（その 7）

【図 24】

本発明の第 2 の実施形態におけるセキュアカードのセキュア領域の構成を示す図

【図 25】

本発明の第 2 の実施形態におけるセキュアカードの AP 管理テーブルの構成を示す図

【図 26】

本発明の第3の実施形態におけるセキュアカードのデータ参照許可指定テーブルを示す図

【図27】

本発明の第3の実施形態におけるセキュアカードのコード使用許可指定テーブルを示す図

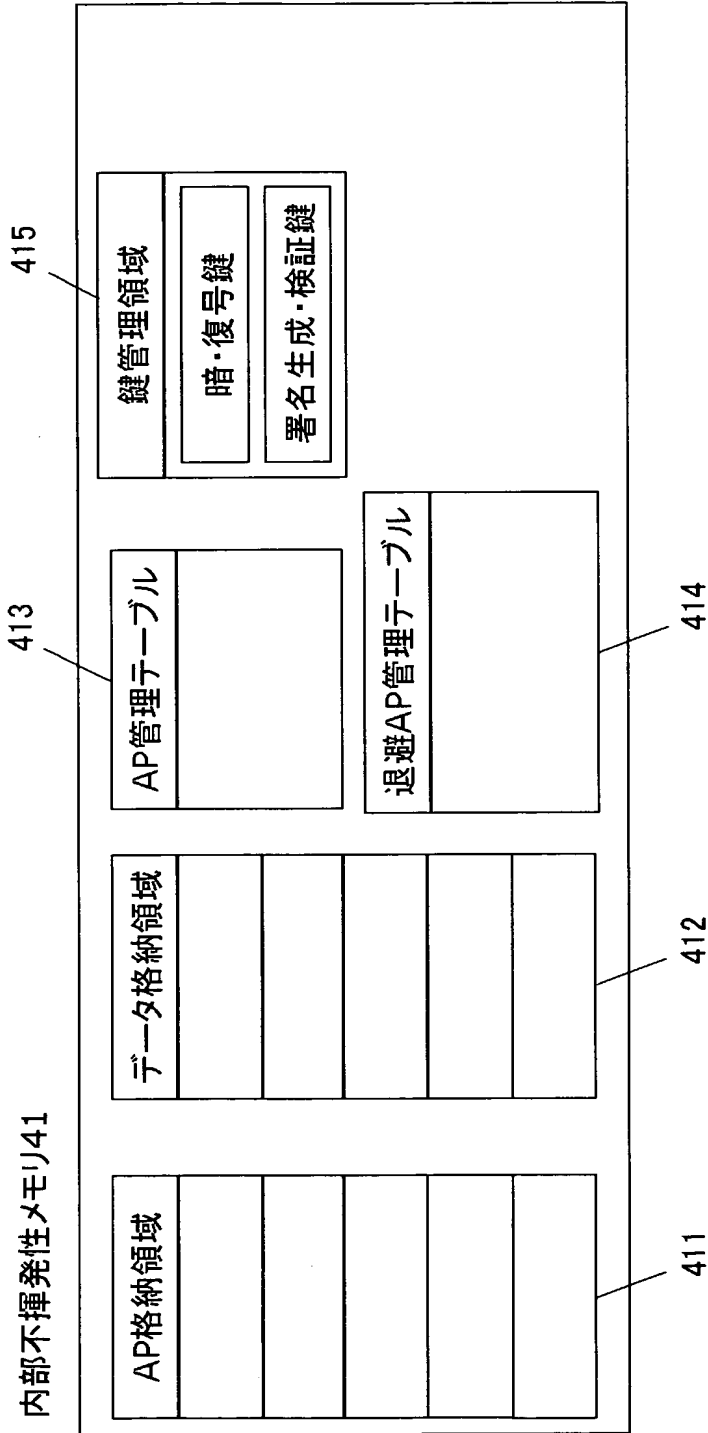
【符号の説明】

- 10 セキュアメモリカード
- 11 IC部
- 12 I/F部
- 13 ICコマンド処理部
- 14 ファイル管理部
- 15 IC認証部
- 16 メモリ管理部
- 17 暗復号回路
- 18 内部不揮発性メモリ I/F部
- 20 制御部
- 21 データ I/F部
- 22 コマンド I/F部
- 23 制御認証部
- 24 コマンド処理部
- 25 アクセス制御部
- 26 大容量不揮発性メモリ I/F部
- 40 TRM
- 41 内部不揮発性メモリ
- 50 大容量不揮発性メモリ
- 51 セキュア領域
- 52 認証領域
- 53 非認証領域
- 60 外部CPU

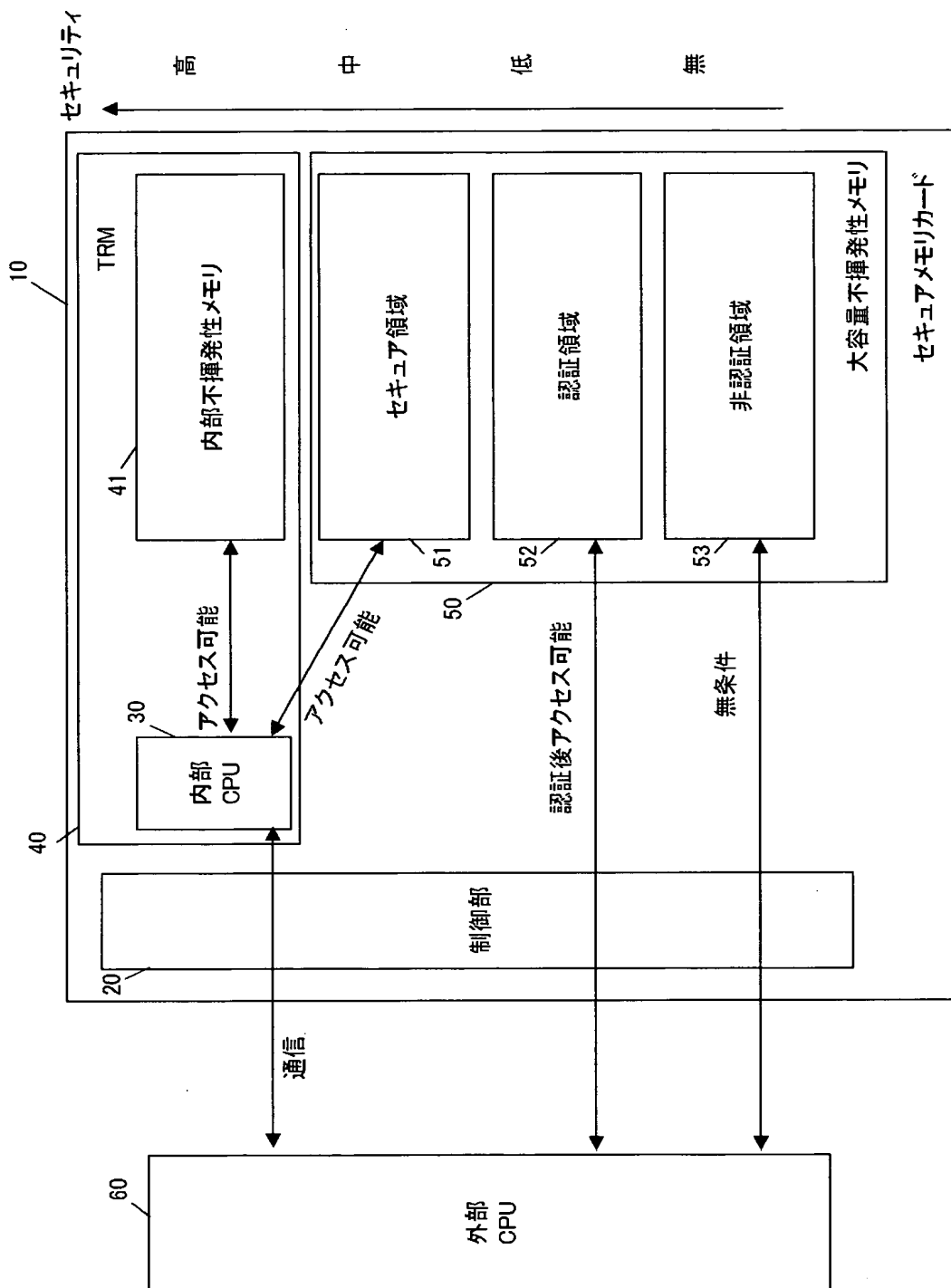
- 4 1 1 AP格納領域
- 4 1 2 データ格納領域
- 4 1 3 AP管理テーブル
- 4 1 4 退避AP管理テーブル
- 4 1 5 鍵管理領域
- 4 1 6 セキュア領域DLAP管理テーブル
- 5 1 1 データ退避領域
- 5 1 2 AP保存領域

【書類名】 図面

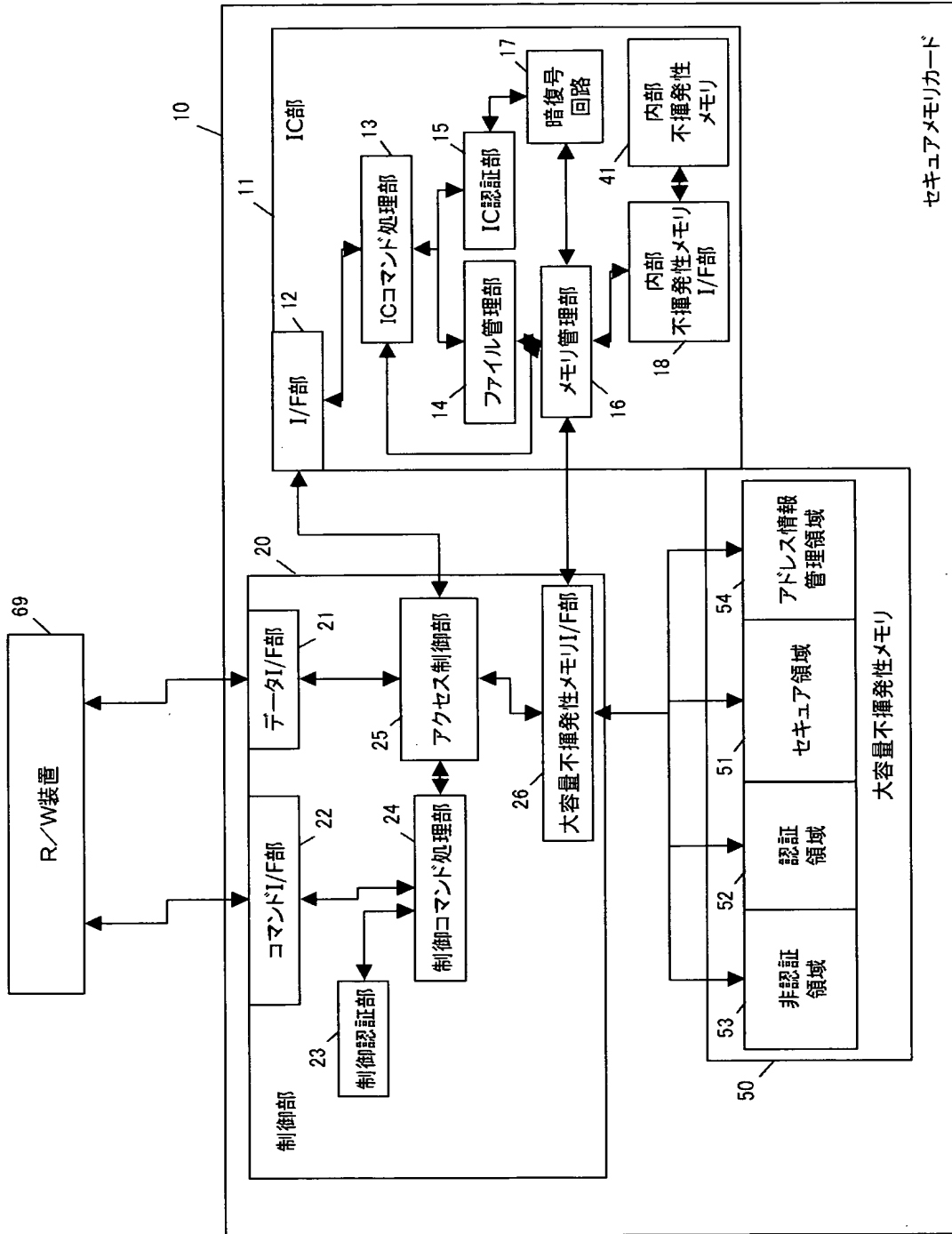
【図 1】



【図 2】



【図3】



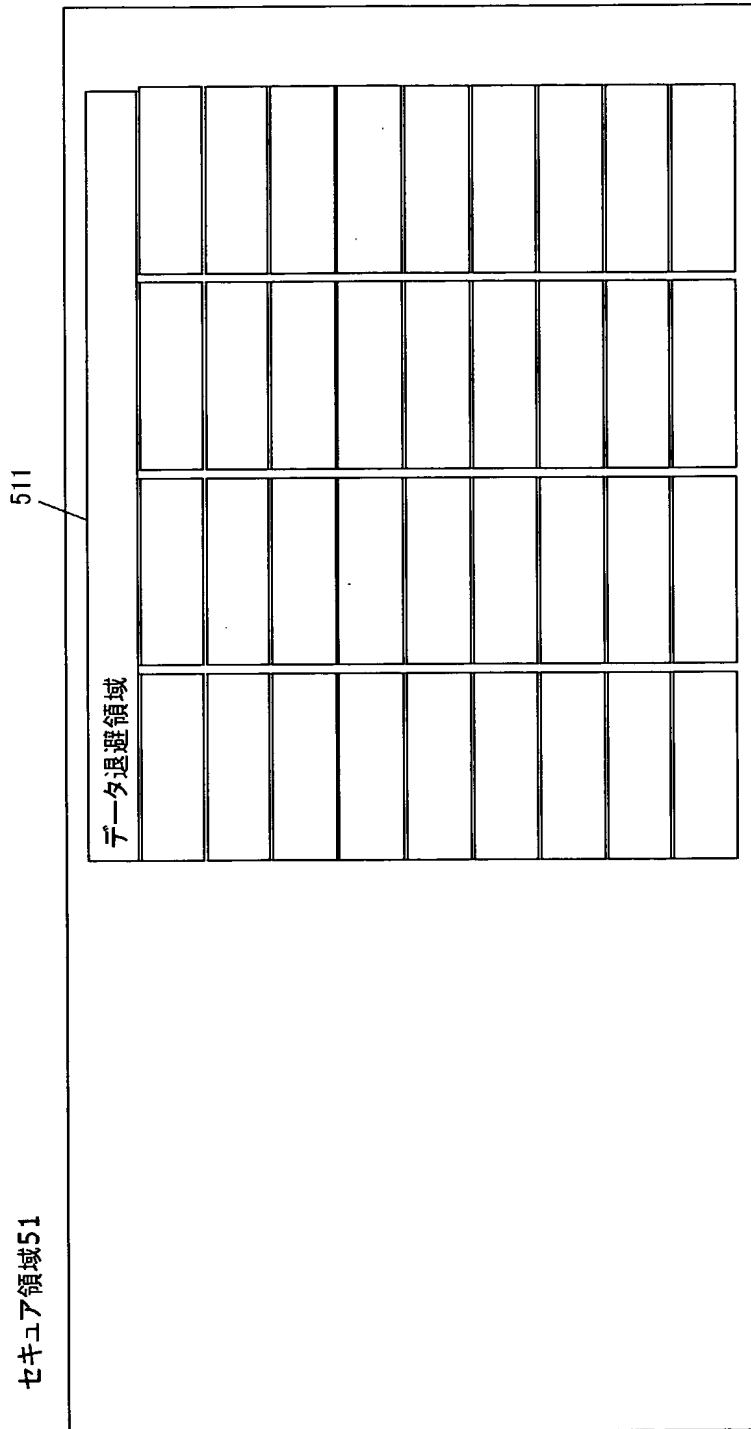
【図4】

#1	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#2	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#3	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#4	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#5	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否

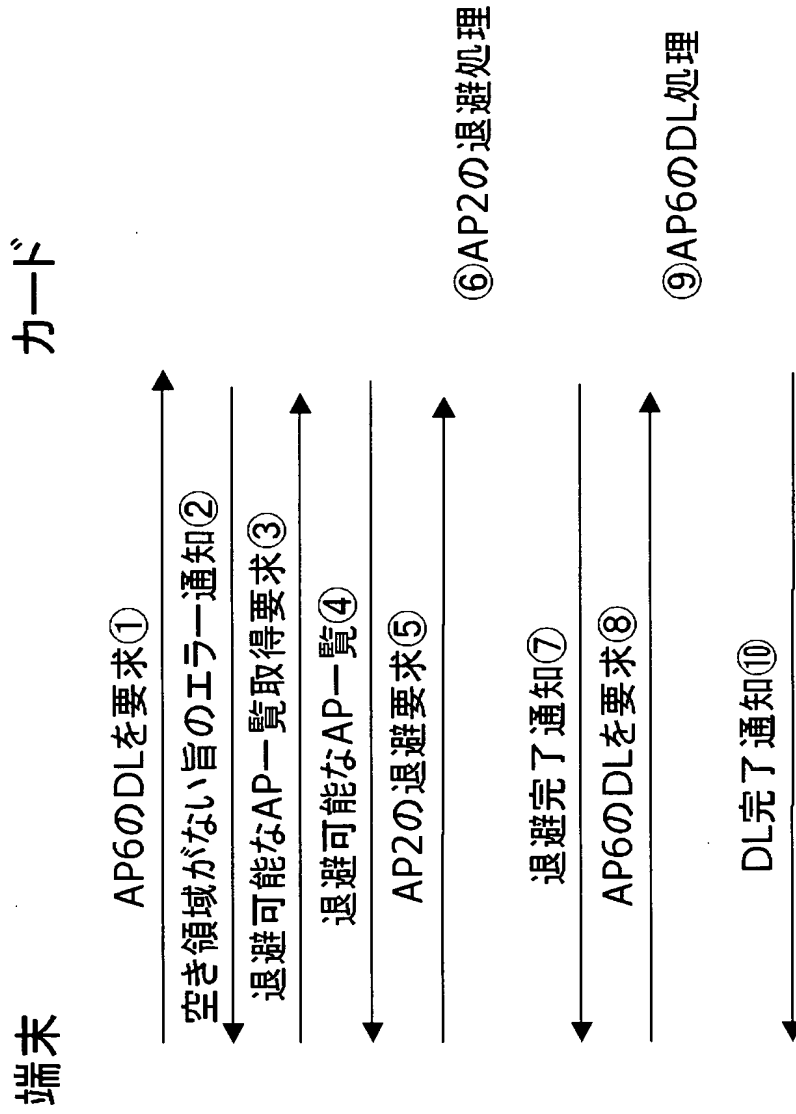
【図 5】

AP識別子	退避データ識別子	署名データ
AP識別子	退避データ識別子	署名データ
AP識別子	退避データ識別子	署名データ
AP識別子	退避データ識別子	署名データ

【図6】



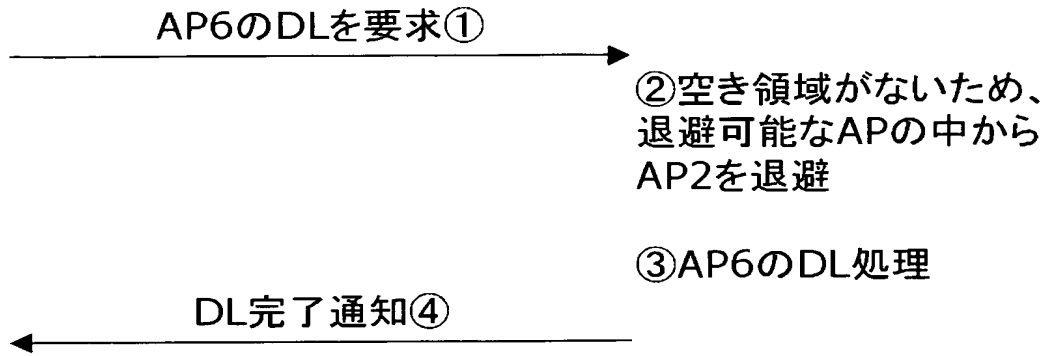
【図7】



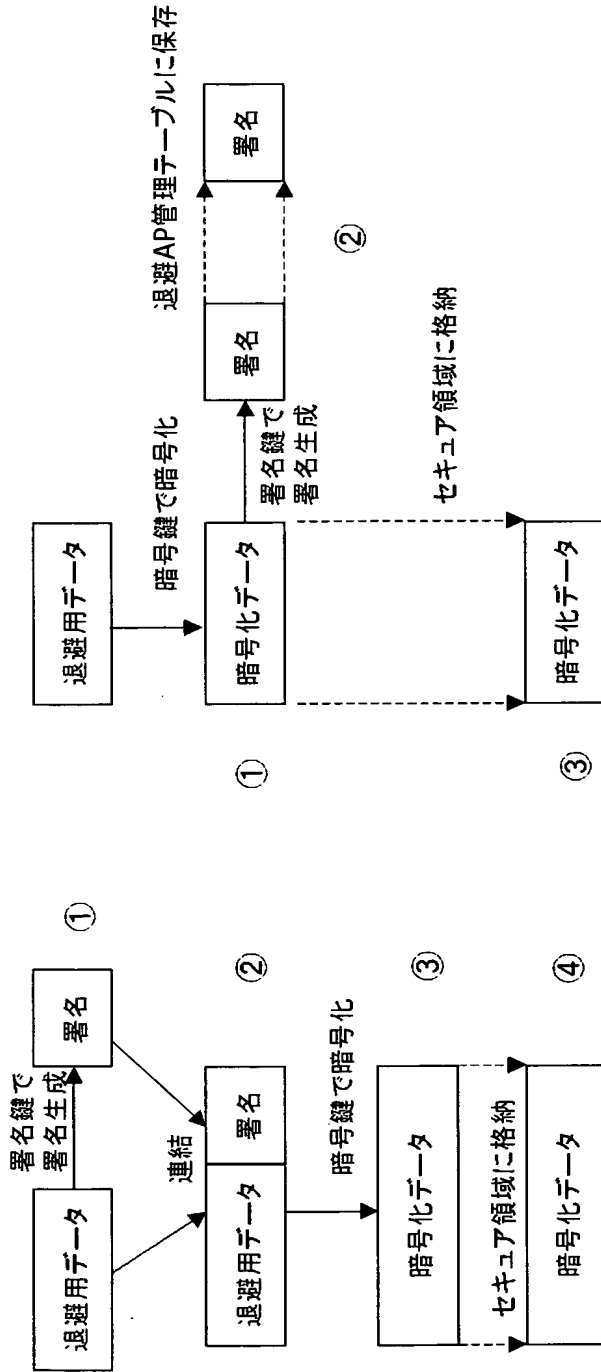
【図8】

端末

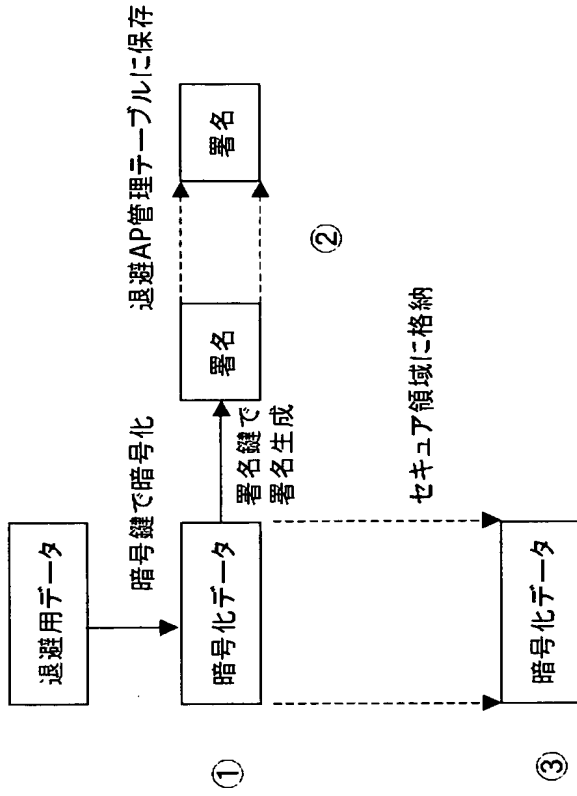
カード



【図 9】

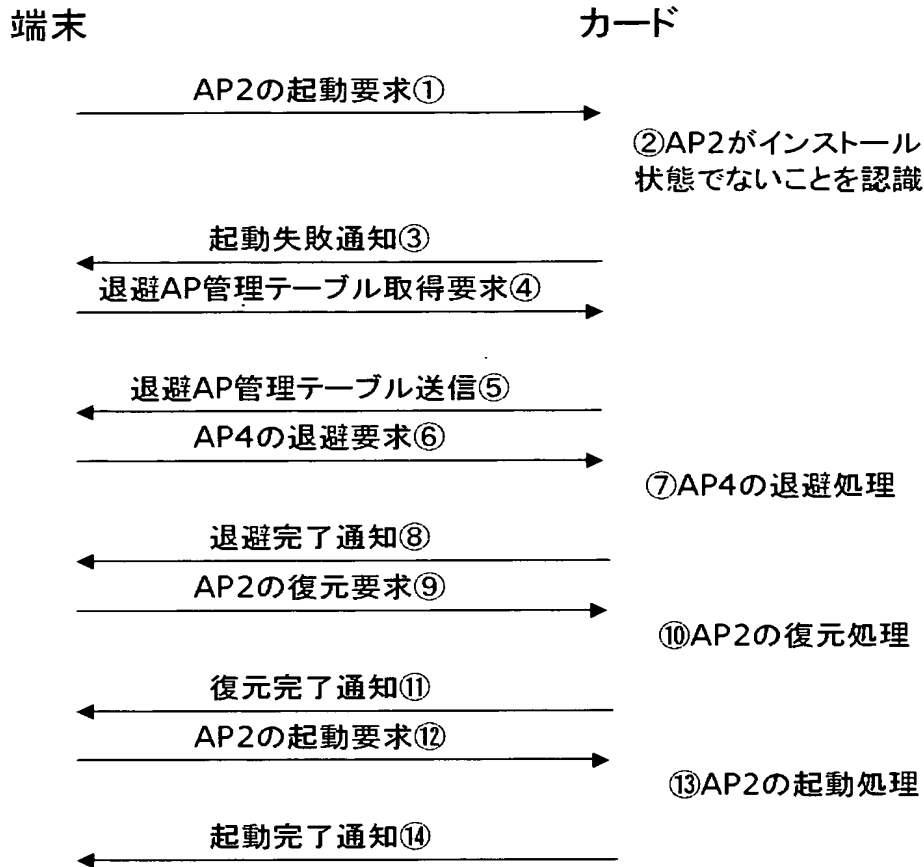


(a)

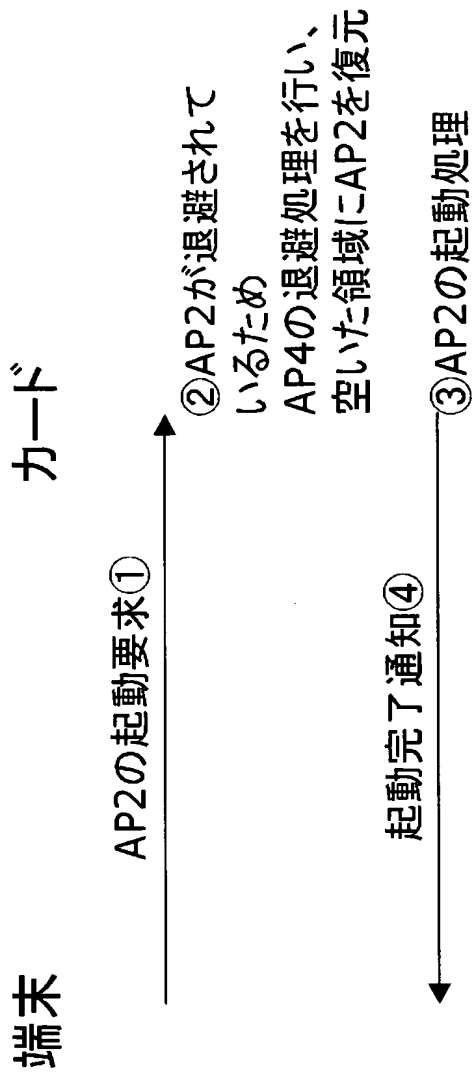


(b)

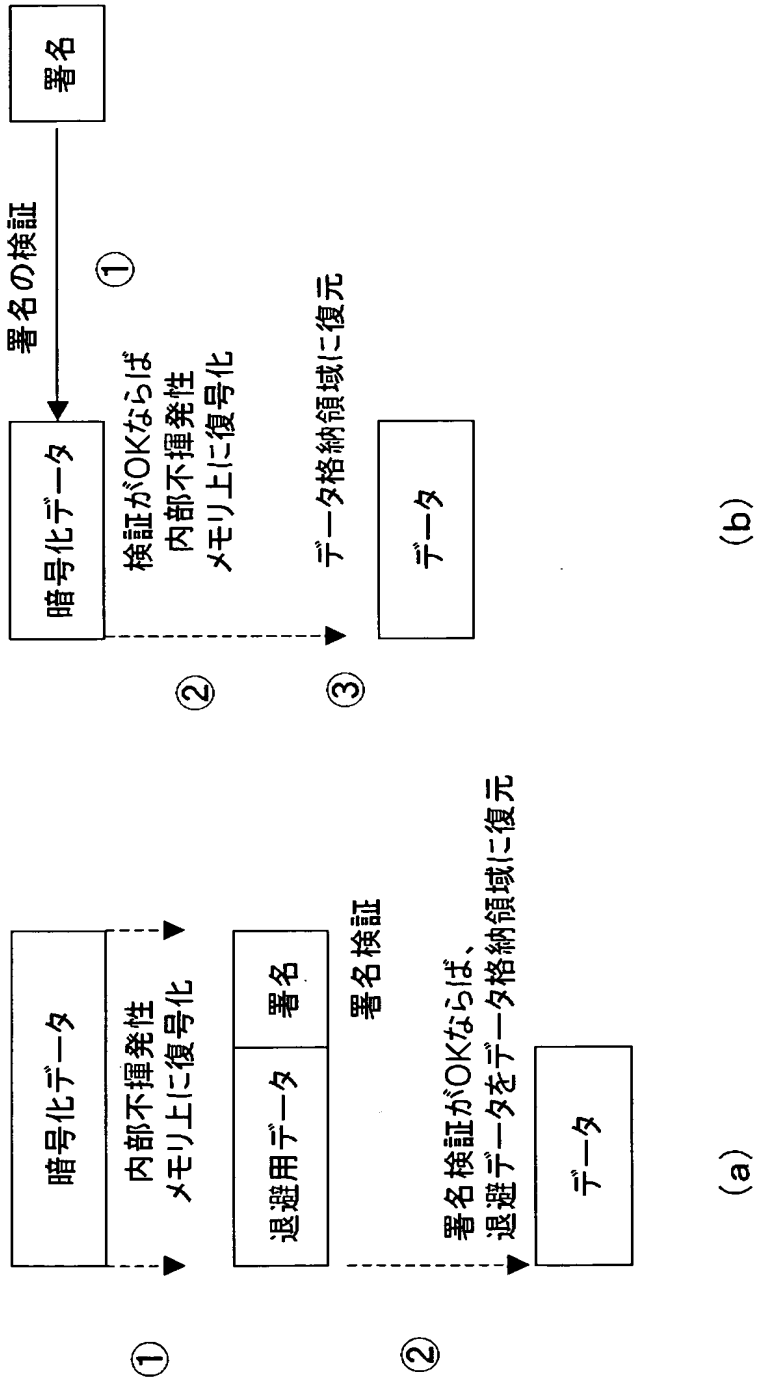
【図 10】



【図11】



【図12】



【図 13】

#1	null	null	null	null	null
#2	null	null	null	null	null
#3	null	null	null	null	null
#4	null	null	null	null	null
#5	null	null	null	null	null

(a)

#1	AP1	no	code1	null	yes
#2	null	null	null	null	null
#3	null	null	null	null	null
#4	null	null	null	null	null
#5	null	null	null	null	null

(b)

#1	AP1	no	code1	null	yes
#2	AP2	no	code2	null	yes
#3	null	null	null	null	null
#4	null	null	null	null	null
#5	null	null	null	null	null

(c)

【図14】

#1	AP1	yes	code1	data1	yes
#2	AP2	yes	code2	data2	yes
#3	null	null	null	null	null
#4	null	null	null	null	null
#5	null	null	null	null	null

(d)

#1	AP1	yes	code1	data1	yes
#2	AP2	yes	code2	data2	yes
#3	AP3	yes	code3	data3	no
#4	AP4	yes	code4	data4	yes
#5	AP5	yes	code5	data5	yes

(e)

【図 15】

#1	AP1	yes	code1	data1	yes
#2	null	null	null	null	null
#3	AP3	yes	code3	data3	no
#4	AP4	yes	code4	data4	yes
#5	AP5	yes	code5	data5	yes

(f)

#1	AP1	yes	code1	data1	yes
#2	AP6	no	code6	null	no
#3	AP3	yes	code3	data3	no
#4	AP4	yes	code4	data4	yes
#5	AP5	yes	code5	data5	yes

(g)

#1	AP1	yes	code1	data1	yes
#2	AP6	no	code6	null	no
#3	AP3	yes	code3	data3	no
#4	AP2	yes	code7	data7	yes
#5	AP5	yes	code5	data3	yes

(h)

【図 16】

(c)

AP2	evac2	sign2
AP4	evac4	sign4
null	null	null
null	null	null

(d)

null	null	null
AP4	evac4	sign4
null	null	null
null	null	null

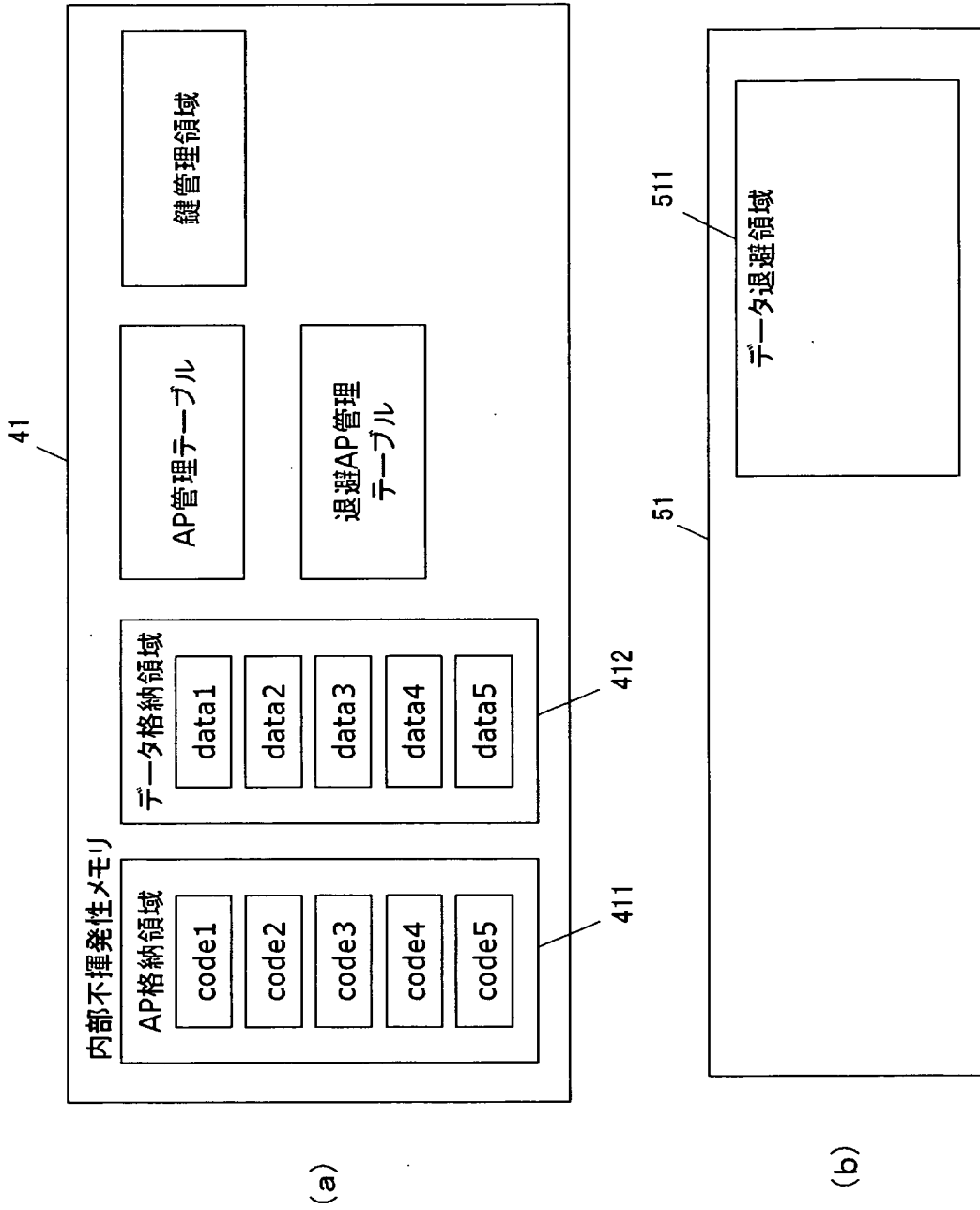
(a)

null	null	null
null	null	null
null	null	null
null	null	null

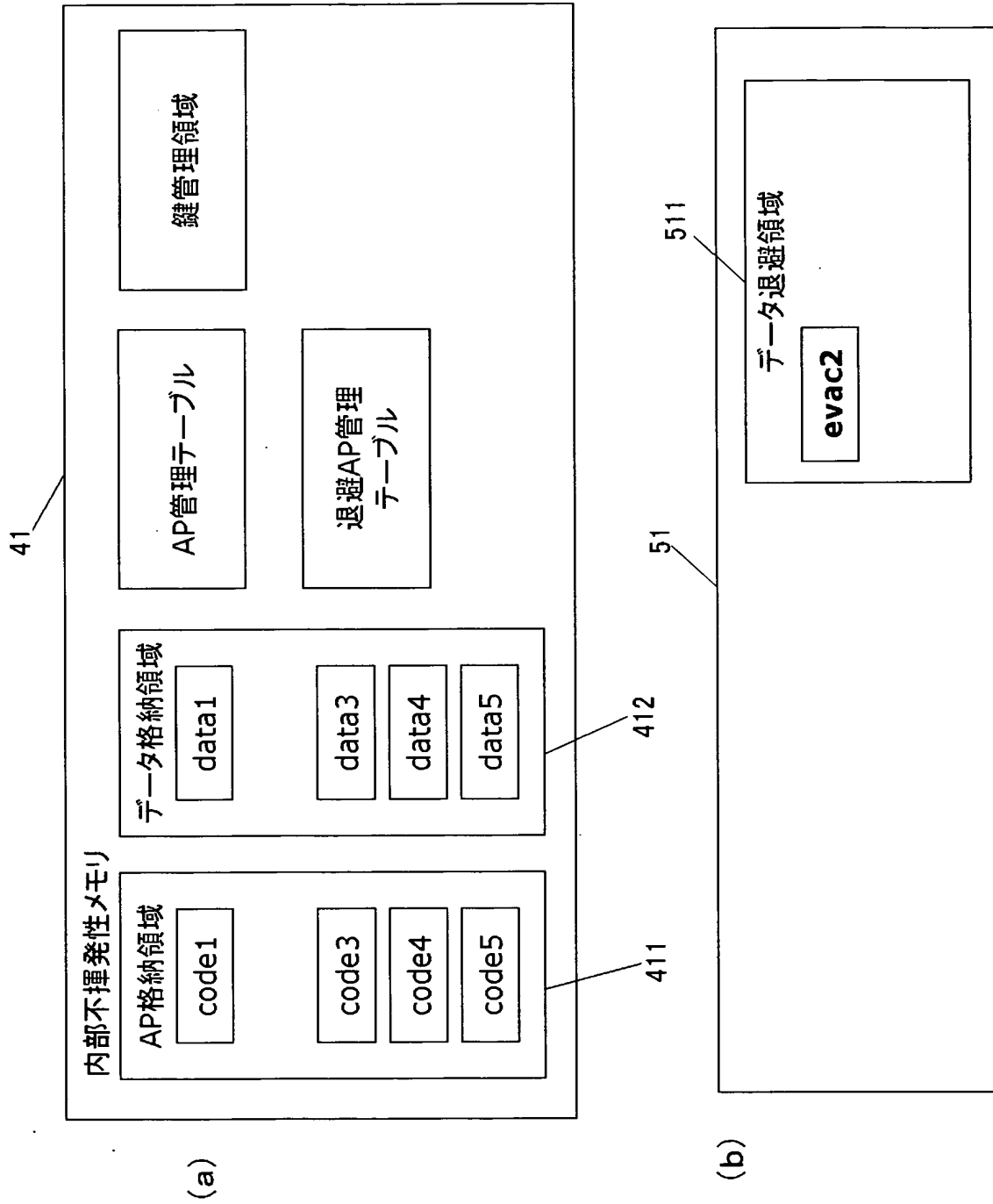
(b)

AP2	evac2	sign2
null	null	null
null	null	null
null	null	null

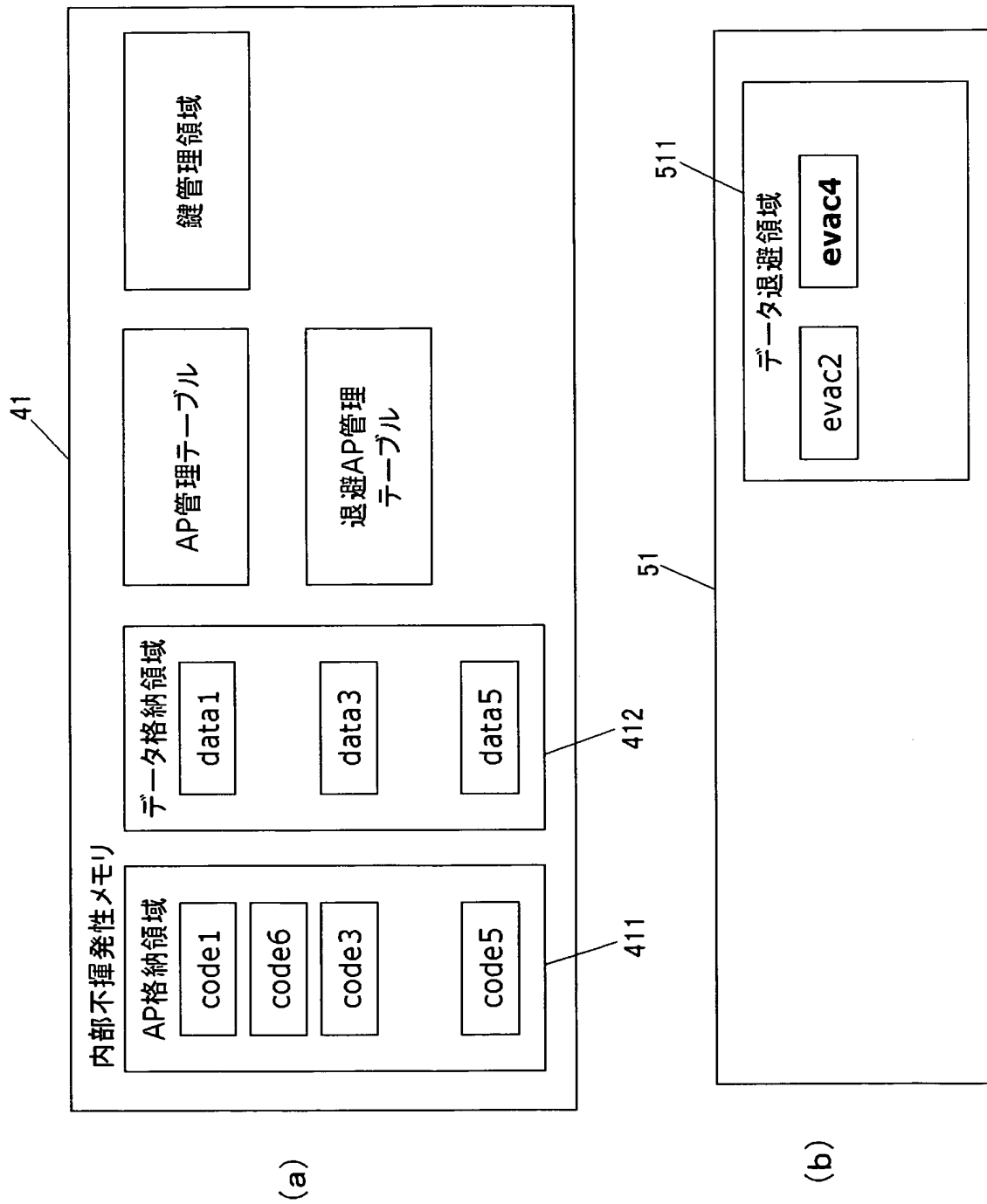
【図17】



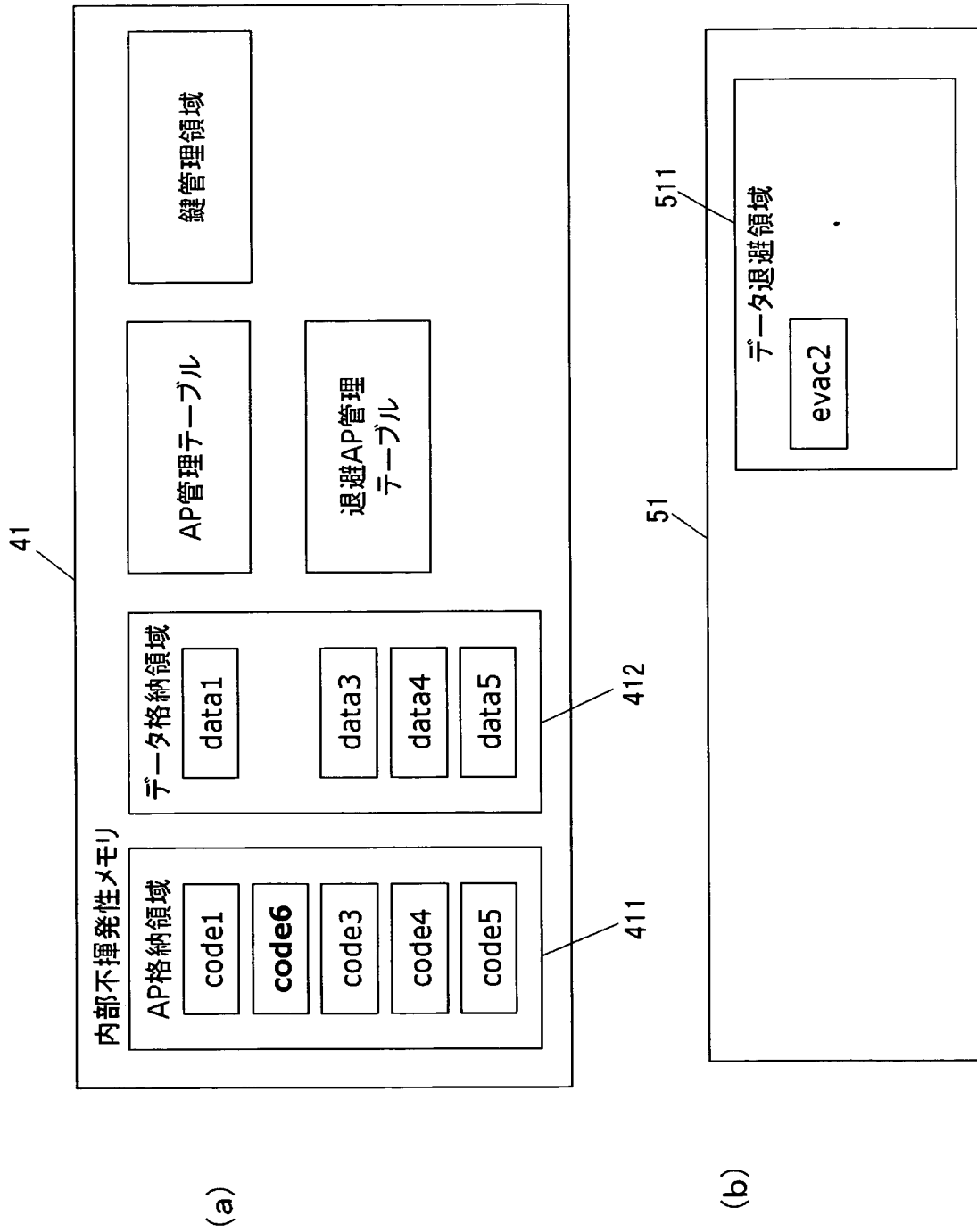
【図18】



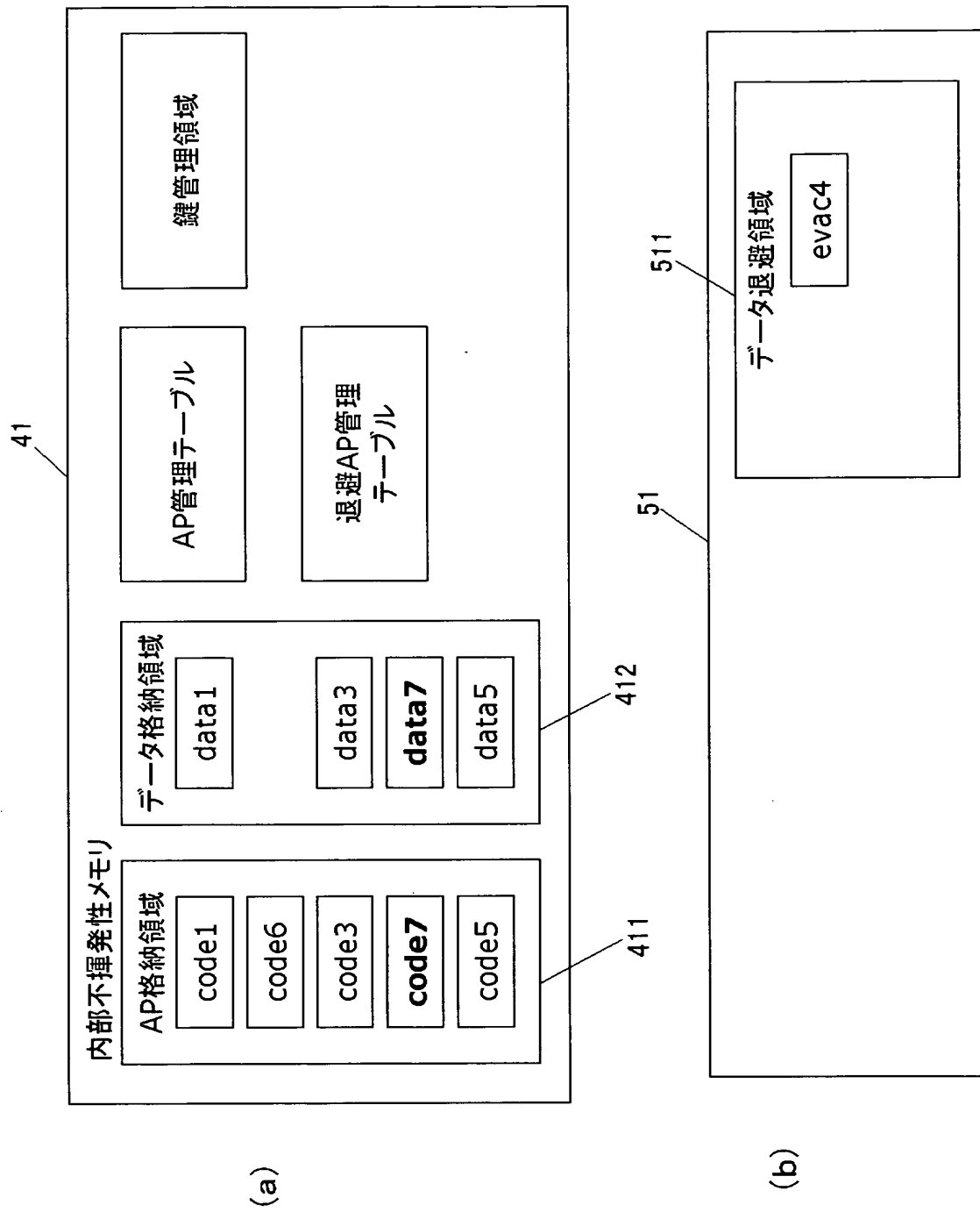
【図19】



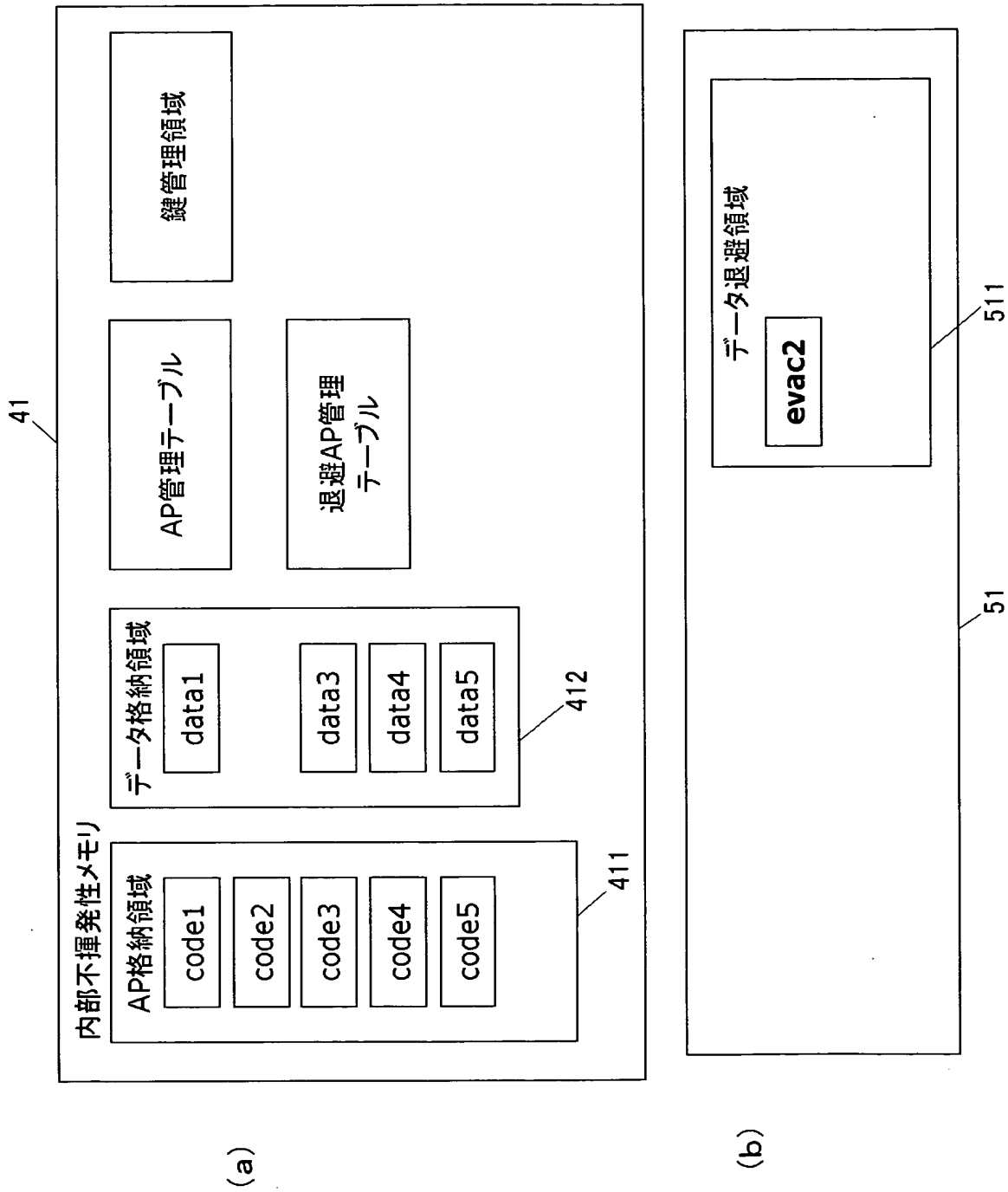
【図 20】



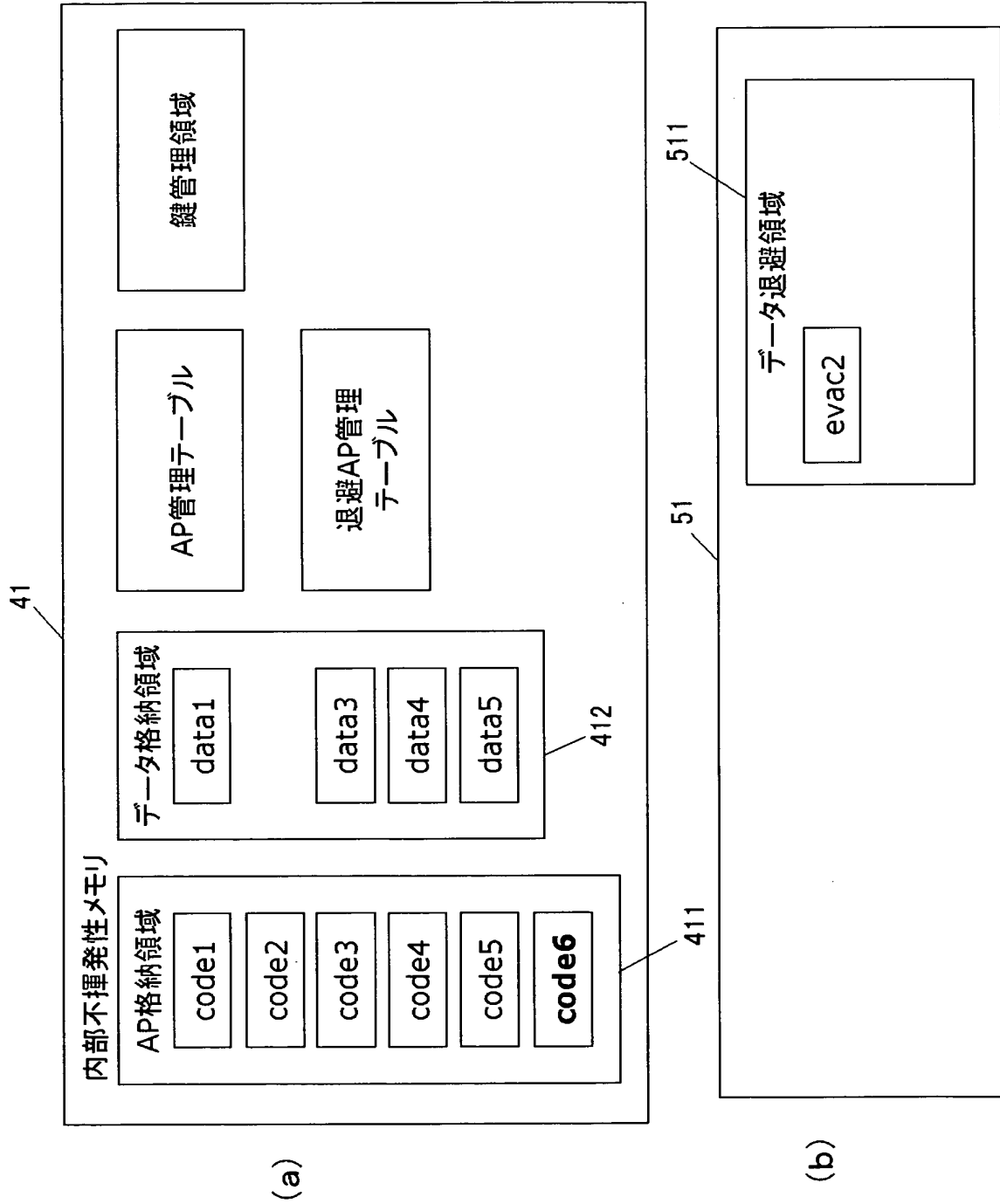
【図 21】



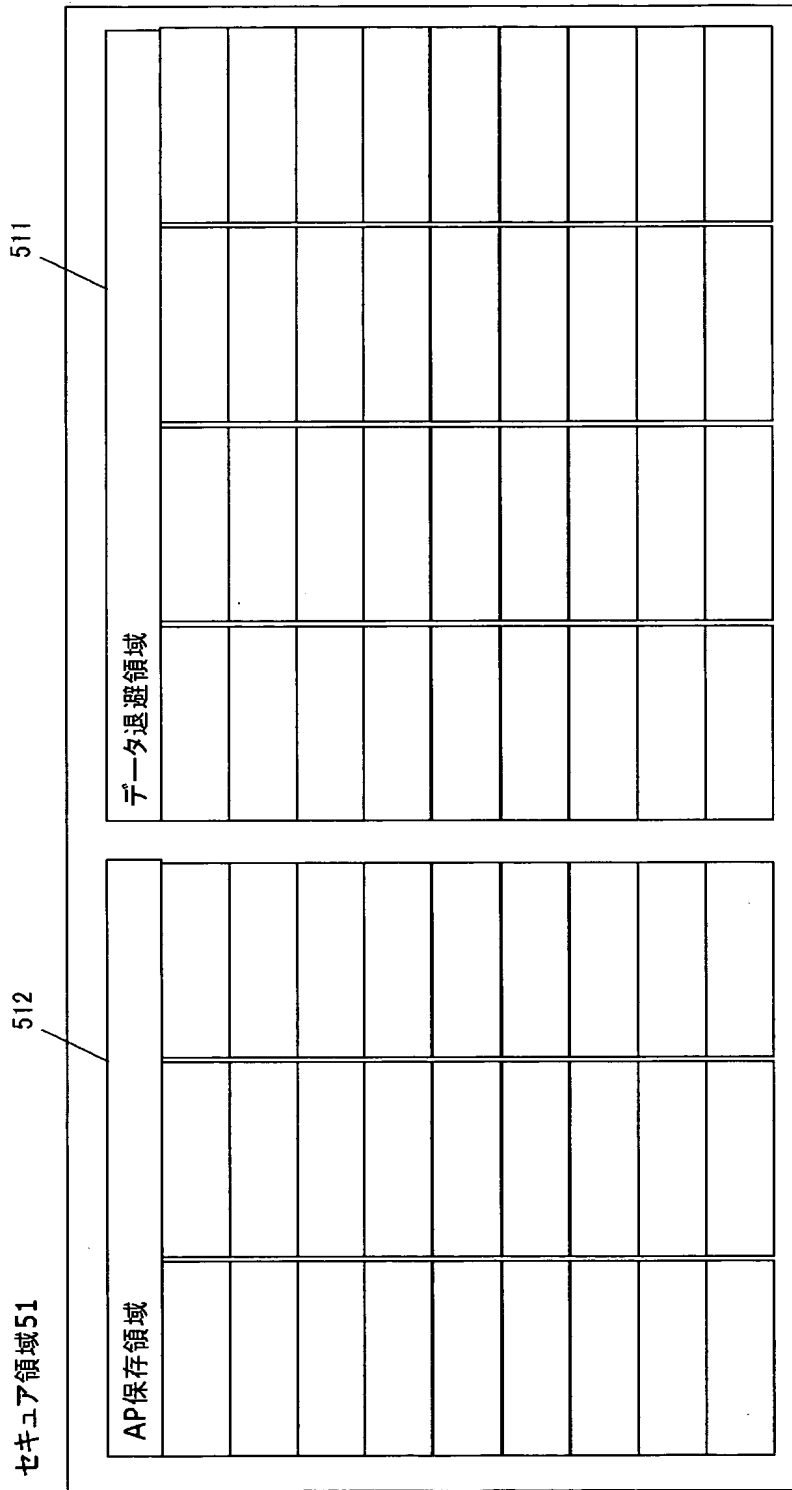
【図22】



【図 23】



【図 24】



【図 25】

#1	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#2	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#3	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#4	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否
#5	AP識別子	インストールフラグ	コードアドレス	データアドレス	回避可否

413

セキュア領域DL AP管理テーブル

#1	AP識別子	格納アドレス	署名データ	回避可否
#2	AP識別子	格納アドレス	署名データ	回避可否
#3	AP識別子	格納アドレス	署名データ	回避可否
#4	AP識別子	格納アドレス	署名データ	回避可否
#5	AP識別子	格納アドレス	署名データ	回避可否
#6	AP識別子	格納アドレス	署名データ	回避可否

416

...

【図 26】

許可指定テーブル

(a)

あるAPが管理するデータ全体	
データ	許可対象AP
データ	許可対象AP
データ	許可対象AP
...	許可対象AP

使用例

(b)

AP2が管理するデータ全体	
data_a	AP1
data_b	null
data_c	AP3
...	...

【図 27】

許可指定テーブル

(a)

あるAPのコード全体	
コード	許可対象AP
コード	許可対象AP
コード	許可対象AP
...	許可対象AP

使用例

(b)

AP2のコード全体	
code_a	AP1
code_b	null
code_c	AP3
...	...

【書類名】 要約書

【要約】

【課題】 APの利用に必要な多くのデータを内部で安全に保持することができるメモリデバイスを提供する。

【解決手段】 電子機器から直接アクセスすることができない耐タンパー性の第1のメモリ41と、電子機器から直接アクセスすることができない非耐タンパー性の第2のメモリとを設け、第2のメモリを使用して、第1のメモリ41に蓄積されたデータを退避するように構成している。このメモリデバイスでは、多数のAPの利用に必要なデータをデバイス内部で安全に保持することができるため、認証条件を満たす端末であれば、どの端末でも、そこに保持されたデータを利用することができる。

【選択図】 図1



特願 2003-042288

出願人履歴情報

識別番号

[000005821]

1. 変更年月日
[変更理由]
住所
氏名

1990年 8月28日
新規登録
大阪府門真市大字門真1006番地
松下電器産業株式会社